UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/683,943 | 03/05/2002 | Christopher L. Parmelee | D-1154R2 | 5493 |

28995 7590 06/01/2007

RALPH E. JOCKE
walker & jocke LPA
231 SOUTH BROADWAY
MEDINA, OH 44256

| EXAMINER |
|---|
| KHOSHNOODI, NADIA |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2137 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/01/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

## BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/683,943
Filing Date: March 05, 2002
Appellant(s): PARMELEE ET AL.

Ralph E. Jocke
For Appellant

## EXAMINER'S ANSWER

This is in response to the appeal brief filed 1/17/2007 appealing from the Office action mailed 4/26/2006.

**(1) Real Party in Interest**

A statement identifying by name the real party in interest is contained in the brief.

**(2) Related Appeals and Interferences**

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal. Appellants noted Application No. 09/683,944 in the Appeal Brief, however Examiner would like to note that the application is no longer on appeal before the Board.

**(3) Status of Claims**

The statement of the status of claims contained in the brief is correct.

**(4) Status of Amendments After Final**

The appellant's statement of the status of amendments after non-final rejection contained in the brief is correct.

**(5) Summary of Claimed Subject Matter**

The summary of claimed subject matter contained in the brief is correct.

**(6) Grounds of Rejection to be Reviewed on Appeal**

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

**(7) Claims Appendix**

The copy of the appealed claims contained in the Appendix to the brief is correct.

### (8) Evidence Relied Upon

| | | |
|---|---|---|
| 2002/0026575 | Wheeler et al. | 02-2002 |
| WO 00/55793 | Cohen | 09-2000 |
| 5,974,146 | Randle et al. | 10-1999 |
| 2004/0215566 | Meurer | 10-2004 |
| 60/223,076 | Wheeler et al. | Provisional Application |

### (9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

The Examiner reviewed the provisional application to point out where the elements relied upon, i.e. paragraphs [108]-[118], [120], [129]-[132], [145], [170], [172], and [182]-[190], in the Wheeler et al. publication are supported in the provisional application.

As per Paragraph [108]:

The Wheeler et al. portions relied upon, i.e. lines 4-9 and 12-15, are supported on pages 5-6 of the "Aads" portion of the provisional.

As per Paragraph [109]:

The Wheeler et al. portions relied upon, i.e. lines 1-5 and 9-11, are supported on page 6 of the "Aads" portion of the provisional and on page 1 of the "Aadsstraw" portion of the provisional.

As per Paragraph [110] – [113]:

The Wheeler et al. portions relied upon, i.e. par. 113 lines 8-12, are supported on page 6 of the "Rachip" portion of the provisional. Furthermore, par. 113 lines 12-18 are supported on pages 1-3 of the "Aadsstraw" portion of the provisional.

As per Paragraph [114]:

The Wheeler et al. portions relied upon, i.e. lines 6-16, are supported on page 5 of the " "Aadsstraw" portion of the provisional.

As per Paragraph [115]:

The Wheeler et al. portions relied upon, i.e. lines 9-20, are supported on pages 12-13 of the "Aadsstraw" portion of the provisional and on page 2 of the "Aadsbrnd" portion of the provisional.

As per Paragraph [117]:

The Wheeler et al. portions relied upon, i.e. lines 1-5 and 9-11, are supported on page 6 of the "Aads" portion of the provisional and on page 1 of the "Aadsstraw" portion of the provisional.

As per Paragraph [118]:

The Wheeler et al. portions relied upon, i.e. lines 1-38, are supported on page 13 of the "Aadsstraw" portion of the provisional. Support of multiple accounts is evident based on the fact that the provisional allows for multiple applications in correspondence with a public key.

As per Paragraph [120]:

The Wheeler et al. portions relied upon, i.e. lines 1-13, are supported on page 13 of the "Aadsstraw" portion of the provisional.

As per Paragraph [129]:

The Wheeler et al. portions relied upon, i.e. lines 1-5, are supported on page 6 of the "Aads" portion of the provisional.

As per Paragraphs [130]-[131]:

The Wheeler et al. portions relied upon, i.e. lines 10-24, are supported on pages 3 & 6 of the "Aadsstraw" portion of the provisional and on page 2 of the "Rachip" portion of the provisional.

As per Paragraph [132]:

The Wheeler et al. portions relied upon, i.e. lines 1-12 are supported on page 2 of "Aadsbrnd" portion of the provisional and on page 6 of the "Aadsstraw" portion of the provisional.

As per Paragraph [145]:

The Wheeler et al. portions relied upon, i.e. lines 1-6, are supported on page 1 of the "Aadsstraw" portion of the provisional.

As per Paragraph [170]:

The Wheeler et al. portions relied upon, i.e. lines 1-12, are supported on pages 3-6 of the "Aadsstraw" portion of the provisional.

As per Paragraph [172]:

The Wheeler et al. portions relied upon, i.e. lines 1-13, are supported on page 6 of the "Aadsstraw" portion of the provisional.

As per Paragraph [182]-[183]:

The Wheeler et al. portions relied upon, i.e. par. 183 lines 1-12, are supported on page 3 of the "Aads" portion of the provisional. Furthermore, par 183 lines 12-18 are supported on page 6 of the "Aadsstraw" portion of the provisional.

As per Paragraph [184]:

The Wheeler et al. portions relied upon, i.e. lines 4-6, are supported on page 5 of the "Aads" portion of the provisional. Furthermore, lines 6-18 are supported on pages 13-14 (from the bottom of page 13) of the "Aadsstraw" portion of the provisional.

As per Paragraph [185]:

The Wheeler et al. portions relied upon, i.e. lines 1-11, are supported on page 12 of the "Aadsstraw" portion of the provisional.

As per Paragraph [186]:

The Wheeler et al. portions relied upon, i.e. lines 1-5, are supported on pages 12-13 (from the bottom of page 12) of the "Aadsstraw" portion of the provisional.

As per Paragraph [187]:

The Wheeler et al. portions relied upon, i.e. lines 1-17, are supported on page 12 of the "Aadsstraw" portion of the provisional.

As per Paragraph [188]:

The Wheeler et al. portions relied upon, i.e. lines 1-8, are supported on pages 4-5 (from the bottom of page 4) of the "Aadsstraw" portion of the provisional.

As per Paragraph [189]:

The Wheeler et al. portions relied upon, i.e. lines 9-15, are supported on page 1 of the "Aadsstraw" portion of the provisional.

As per Paragraph [190]:

The Wheeler et al. portions relied upon, i.e. lines 1-8, are supported on page 6 of the "Aadsstraw" portion of the provisional and pages 1-2 of the "Aadsbrnd" portion of the provisional.

Applicants further contend that the provisional application of the Meurer reference was not supportive of paragraph [013]. Thus, the Examiner has reviewed the provisional application to point out where the elements relied upon in the Wheeler et al. publication are supported in the provisional application.

As per Paragraph [013]:

The Meurer portion relied upon is supported on pages 42-43 of the provisional application.

Based on the above details listing it is evident that each of the paragraphs relied upon are supported by specific details as set forth in their corresponding provisional applications. Thus, the non-final rejection as set forth in the previous office action has been maintained in light of the cited pages which show that the provisional date is effective. Furthermore, the provisional applications of each of the references relied upon has been cited and mailed along with this office action to ensure that the Applicants are able to review the cited portions.

## *Claim Objections*

Claims 1-5, 9-11, 13-15, 18, and 31-32 are objected to because of the following informalities:

These claims use the acronym "ATM" where when using an acronym in a claim, Applicants must first spell out what the acronym stands for and can then use the acronyms for latter references made. For example, in each of the independent claims that use "ATM" Applicants can rewrite the first reference to an "ATM" to include "automated transaction machine (ATM)."

### ***Claim Rejections - 35 USC § 103***

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**II. Claims 1-6, 8-11, 15-16, 19, 27-30, 33-39, and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al., United States Pub. No. 2002/0026575 and further in view of Cohen, WO 00/55793.**

**As per claim 1:**

Wheeler et al. substantially teach an apparatus comprising: at least one computer processor; and at least one data store in operative connection with the computer processor, wherein the at least one data store includes a plurality of digital accounts stored therein, wherein each of the digital accounts is associated with at least one private key (par. 113), wherein the computer processor is operative to communicate with a plurality of ATMs, wherein the computer processor is operative responsive to at least one of the ATMs to cause a digital signature to be produced for an electronic document responsive to the private key associated with one of the digital accounts (par. 109).

Not explicitly disclosed is a digital safe deposit account. However, Cohen teaches the use of an electronic safety deposit box (page 12, lines 7-14). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. for the digital account to be a digital safe deposit account. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Cohen suggests that using an electronic safety deposit box allows for quick and authenticated access to important user documents/records on page 12, lines 7-14.

**As per claim 2:**

Wheeler et al. and Cohen substantially teach the apparatus according to claim 1. Not explicitly disclosed is wherein the computer processor is operative to receive the electronic document from the at least one ATM, wherein the computer processor is operative to store the electronic document in the data store in association with the one digital safe deposit account. However, Wheeler et al. teach that the electronic document may be stored (par. 170). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to store the electronic document in the data stored in association with the one digital safe deposit account. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Wheeler et al. suggest that messages used in various financial transactions may be stored in par. 170.

**As per claim 3:**

Wheeler et al. and Cohen substantially teach the apparatus as applied to claim 2 above. Furthermore, Cohen et al. teach the apparatus wherein the computer processor is operative to retrieve the electronic document from the data store and send the electronic document to any one of the plurality of ATMs (page 12, lines 7-14).

**As per claim 4:**

Wheeler et al. and Cohen substantially teach the apparatus according to claim 2. Furthermore, Wheeler et al. teach wherein the computer processor is operative to encrypt and decrypt the electronic document stored in the at least one data store responsive to a secret key received from the at least one ATM (par. 117).

**As per claim 5:**

Wheeler et al. and Cohen substantially teach the apparatus as applied to claim 1 above. Furthermore, Wheeler et al. teach the apparatus wherein each digital safe deposit account is associated with a financial account number, wherein the computer processor is operative to access the private key associated with the one digital safe deposit account responsive to a message received from the at least one ATM which includes a financial account number that corresponds to the financial account number associated with the one digital safe deposit account (par. 189-190).

**As per claim 6:**

Wheeler et al. and Cohen substantially teach the apparatus as applied to claim 5 above. Furthermore, Wheeler et al. teach the apparatus wherein the at least one financial account number corresponds to a credit card number (par. 183).

**As per claim 8:**

Wheeler et al. and Cohen substantially teach the apparatus as applied to claim 1 above. Furthermore, Wheeler et al. teach the apparatus wherein the computer processor is operative to maintain and store in the at least one data store, an access log in association with each digital safe deposit account (par. 120).

**As per claim 9:**

Wheeler et al. and Cohen substantially teach the apparatus as applied to claim 1 above. Furthermore, Wheeler et al. teach the apparatus wherein the at least one ATM includes a cash dispenser, wherein the computer processor is operative through communication with a financial transaction processing system to cause a dispense of cash from the cash dispenser to be authorized (par. 183).

**As per claim 10:**

Wheeler et al. and Cohen substantially teach the apparatus as applied to claim 1 above. Furthermore, Wheeler et al. teach the apparatus wherein the computer processor is operative to cause a new digital safe deposit account to be created in the data store responsive to communication from the at least one ATM (par. 129-132).

**As per claim 11:**

Wheeler et al. and Cohen substantially teach the apparatus according to claim 10. Furthermore, Wheeler et al. teach the apparatus wherein the computer processor is operative to cause a new private key and a corresponding public key to be produced responsive to communication from the at least one ATM, wherein the computer processor is operative to store the private key in association with the new digital safe deposit account (par. 108-113).

**As per claim 15:**

Wheeler et al. and Cohen substantially teach the apparatus according to claim 1. Furthermore, Wheeler et al. teach the apparatus wherein the computer processor is operative to receive a one-way hash of the electronic document from the at least one ATM, wherein the computer processor is operative to cause the digital signature to be generated responsive to the one-way hash and the private key (par. 145).

**As per claim 16:**

Wheeler et al. and Cohen substantially teach the apparatus according to claim 1. Not explicitly disclosed is wherein the computer processor is operative to cause a second digital signature to be produced for the electronic document responsive to a private key that is not associated with the one digital safe deposit account. However, Wheeler et al. teach that there can be more than one account per person and that each account can have its own public/private key pair (par. 118). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to have a second signature that is associated with another account. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Wheeler et al. suggest that each account should be unique and should therefore have its own public/private key pair in par. 118.

**As per claim 19:**

Wheeler et al. and Cohen substantially teach the apparatus as applied to claim 1 above. Furthermore, Wheeler et al. wherein the computer processor is operative to cause a digital time stamp to be produced and attached to the electronic document (par. 172).

**As per claim 27:**

Wheeler et al. substantially teach a method comprising: a) receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine, wherein the request includes an account number that is associated with a digital account; b) accessing a private key associated with the digital account responsive to the account number; and c) producing a digital signature for the electronic document responsive to the private key; and d) causing the digital signature to be attached to the electronic document (par. 190).

Not explicitly disclosed is a digital safe deposit account. However, Cohen teaches the use of an electronic safety deposit box (page 12, lines 7-14). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. for the digital account to be a digital safe deposit account. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Cohen suggests that using an electronic safety deposit box allows for quick and authenticated access to important user documents/records on page 12, lines 7-14.

**As per claim 28:**

Wheeler et al. and Cohen substantially teach the method as applied to claim 27 above. Furthermore, Wheeler et al. teach the method, further comprising: e) storing a digitally signed copy of the electronic document in a data store in association with the digital safe deposit account (par 170).

**As per claim 29:**

Wheeler et al. and Cohen substantially teach the method as applied to claim 27 above. Furthermore, Wheeler et al. teach the method, wherein in step (a) the account number corresponds to a financial account number (par. 183).

**As per claim 30:**

Wheeler et al. and Cohen substantially teach the method as applied to claim 27 above. Furthermore, Wheeler et al. teach the method, further comprising: e) dispensing cash from the automated transaction machine (par. 184).

**As per claims 33 and 41:**

Wheeler et al. substantially teach a method and computer readable media with instructions comprising a) receiving, data associated with a financial account; b) responsive to the data associated with the financial account received in (a), causing through operation, a private key which corresponds to the data associated with the financial account received in (a) to be accessed from at least one data store in operative connection with a computer processor, wherein the private key was previously stored in the at least one data store in correlated relation with the data associated with the financial account; c) causing through operation of a computer processor, a digital signature to be produced for an electronic document responsive to the private key accessed in (b); and d) causing through operation of the computer processor, the digital signature to be attached to the electronic document (par. 190).

Not explicitly disclosed is a server for carrying out these operations. However, Cohen teaches that these operations can be carried out via a server (page 16, line 32 – page 17, line 5). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to carry out the operations on a server instead of a smart card with a processor. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Cohen suggests that webbanks may be maintained on a server of the financial institution where it can serve as a miniature private bank on page 16, line 32 – page 17, line 5.

Also not explicitly disclosed is causing through operation of the server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account. However, Wheeler et al. teach, in another embodiment, that the ATM has a display window so that customers can choose from the possible operations (par. 188-189). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to also visually display the message with the attached signature, which includes the operation chosen.

This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Wheeler et al. suggest displaying a menu of accounts available to the account holder, where the possible transaction types are also displayed for the account holder to choose from and the result of the transaction is displayed once the transaction has been performed in par. 188-189.

**As per claim 34:**

Wheeler et al. and Cohen substantially teach the method of claim 33. Furthermore, Wheeler et al. teach the method wherein (a) the data associated with the financial account is representative of a financial account number (par. 183).

**As per claim 35:**

Wheeler et al. and Cohen substantially teach the method of claim 34. Furthermore, Wheeler et al. teach the method wherein (a) the at least one financial account number corresponds to at least one of a credit card number, a debit card number, and a bank account number (par. 183).

**As per claim 36:**

Wheeler et al. and Cohen substantially teach the method of claim 34. Furthermore, Wheeler et al. teach the method wherein (a) the data representative of the financial account number is received by the at least one server from and automated transaction machine in operative communication with the at least one server through a network (par. 114), wherein in (d) the automated transaction machine includes a display (par. 188).

**As per claim 37:**

Wheeler et al. and Cohen substantially teach the method of claim 36. Furthermore, Wheeler et al. teach the method wherein (a) the automated transaction machine includes a cash dispenser (par. 183).

**As per claim 38:**

Wheeler et al. and Cohen substantially teach the method of claim 33. Furthermore, Wheeler et al. teach the method e) receiving with the at least one server, the electronic document; f) causing through operation of the at least one server the electronic document to be stored in the at least one data store in correlated relation with the data associated with the financial account received (par. 170).

**As per claim 39:**

Wheeler et al. and Cohen substantially teach the method of claim 38. Furthermore, Wheeler et al. teach the method further comprising g) subsequent to (f) receiving with the at least one server, data associated with the financial account from a remote computer in operative communication with the at least one server through a network (par. 114). Furthermore, Cohen teaches h) causing through operation of the at least one server the electronic document accessed from the at least one data store responsive to the data associated with the financial account received in (g); I) causing through operation of the at least one server, the electronic document to be communicated to the remote computer (page 12, lines 7-14).

**III. Claims 7, 12-14, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al., United States Pub. No. 2002/0026575 and**

**Cohen, WO 00/55793as applied to claims 1 and 11 above, and further in view of Randle et al., United States Patent No. 5,974,146.**

**As per claim 7:**

Wheeler et al. and Cohen substantially teach the apparatus according to claim 1. Not explicitly disclosed is wherein each digital safe deposit account is associated with at least one digital certificate, wherein the computer processor is operative to cause the digital signature and at least one of the digital certificates associated with the one digital safe deposit account to be attached to the electronic document. However, Randle et al. teach that customers can gain access to resources by using a certificate related to the account (col. 11, lines 20-38). Furthermore, it is well known that a certificate is used to bind an identity to a public key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to cause a digital certificate to be generated and stored in association with the digital safe deposit account. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Randle et al. suggest the use of an account certificate in order to gain access to an account-related services in col. 11, lines 20-38.

**As per claim 12:**

Wheeler et al. and Cohen substantially teach the apparatus according to claim 11. Not explicitly disclosed is wherein the computer processor is operative to cause a digital certificate to be generated and stored in association with the new digital safe deposit account, wherein the digital certificate includes the public key. However, Randle et al. teach that customers can gain access to resources by using a certificate related to the account (col. 11, lines 20-38). Furthermore, it is well known that a certificate is used to bind an identity to a public key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to cause a digital certificate to be generated and stored in association with the digital safe deposit account. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Randle et al. suggest the use of an account certificate in order to gain access to an account-related services in col. 11, lines 20-38.

**As per claim 13**

Wheeler et al. and Cohen substantially teach the apparatus according to claim 12. Furthermore, Wheeler et al. teach wherein the computer processor is operative to receive a financial account number from the at least one ATM, wherein the computer processor is operative to store the financial account number in association with the new digital safe deposit account (par. 184-185).

**As per claim 14:**

Wheeler et al. and Cohen substantially teach the apparatus as applied to claim 13 above. Furthermore, Wheeler et al. teach the apparatus wherein the computer processor is operative to receive a password input from the at least one ATM, wherein the computer processor is operative to store the password input in association with the new digital safe deposit account (par. 187).

**As per claim 40:**

Wheeler et al. and Cohen substantially teach the method of claim 33. Not explicitly disclosed is e) causing through operation of the at least one server at least one digital certificate associated with the private key to be accessed from the at least one data store, wherein the at least one digital certificate was previously stored in the at least one data store in correlated relation with the data associated with the financial account; and f) causing through operation of the at least one server, the at least one digital certificate to be attached to the electronic document during or after the display of the electronic document through the display device.

However, Randle et al. teach that customers can gain access to resources by using a certificate related to the account (col. 11, lines 20-38). Furthermore, it is well known that a certificate is used to bind an identity to a public key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to access the digital certificate that was previously stored in association with the account, as well as to display the document with the attached digital certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Randle et al. suggest the use of an account certificate in order to gain access to an account-related services in col. 11, lines 20-38.

**IV. Claims 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al., United States Pub. No. 2002/0026575 and Cohen, WO**

**00/55793as applied to claim 1 above, and further in view of Meurer, United States Patent Application Publication No. 2004/0215566.**

**As per claim 17:**

Wheeler et al. and Cohen substantially teach the apparatus as applied to claim 1 above. Not explicitly disclosed is the apparatus wherein the computer processor is operative to cause a digital signature processing fee to be assessed to a financial account in response to causing the digital signature to be produced for the electronic document. However, Meurer teaches assessing a processing fee collected for processing transactions (par. 13). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to cause a digital signature processing fee to be assessed to a financial account in response to producing the digital signature for the electronic document. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Meurer suggest assessing a processing fee for various transactions in paragraph 13.

**As per claim 18:**

Wheeler et al. and Cohen substantially teach the apparatus according to claim 17. Furthermore, Wheeler et al. teach the apparatus wherein the computer processor is operative to receive information about the financial account from the at least one ATM (par. 190).

**V. Claims 20-21, 23, 25-26, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al., United States Pub. No. 2002/0026575.**

**As per claim 20:**

Wheeler et al. substantially teach a method comprising: b) accessing a private key and c) enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key (par. 190).

Not explicitly disclosed in that embodiment is a) receiving a financial account number from an automated transaction machine and b) accessing a private key associated with the financial account number. However, in another embodiment, Wheeler et al. teach that an account number is needed in order to utilize the public/private key pair (par. 113). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to receive an account number in order to access the private key associated with the account number in that embodiment as well. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Wheeler et al. suggest that an account is identifiable with a unique identifier such as an account id/number in par. 113.

**As per claim 21:**

Wheeler et al. substantially teach the method, as applied to claim 20 above. Furthermore, Wheeler et al. teach the method wherein prior to step (c) further comprising: d) receiving a password from the automated transaction machine; and e) verifying that the password corresponds to a valid password previously associated with the financial account number (par. 187).

**As per claim 23:**

Wheeler et al. substantially teach the method, as applied to claim 20 above. Furthermore, Wheeler et al. teach the method, further comprising: d) storing a digitally signed copy of the electronic document in a digital safe deposit account in association with the financial account number (par. 170).

**As per claim 25:**

Wheeler et al. substantially teach the method as applied to claim 20 above. Furthermore, Wheeler et al. teach the method further comprising: d) enabling the electronic document to be digitally time stamped (par.  172).

**As per claim 26:**

Wheeler et al. substantially teach the method as applied to claim 20 above. Furthermore, Wheeler et al. teach the method, further comprising: d) dispensing cash from the automated transaction machine (par. 183).

**As per claim 31:**

Wheeler et al. substantially teach a method comprising: a) receiving a request at an ATM to digitally sign an electronic document; b) causing a digital signature and a digital time stamp to be produced for the electronic document; and c) causing the digital signature and the digital time stamp to be attached to the electronic document (par. 115).

Not explicitly disclosed in that embodiment is a) receiving a request at an ATM to digitally sign an electronic document visually displayed by the ATM. However, Wheeler et al. teach, in another embodiment, that the ATM has a display window so that customers can choose from the possible operations (par. 188-189). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to also visually display the message to be signed, which includes the operation chosen. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Wheeler et al. suggest displaying a menu of accounts available to the account holder, where the possible transaction types are also displayed for the account holder to choose from and the result of the transaction is displayed once the transaction has been performed in par. 188-189.

**As per claim 32:**

Wheeler et al. substantially teach the method as applied to claim 31 above. Furthermore, Wheeler et al. teach the method, further comprising: e) dispensing cash from the ATM (par. 184).

**VI. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al., United States Pub. No. 2002/0026575 as applied to claim 20 above, and further in view of Randle et al., United States Patent No. 5,974,146.**

**As per claim 22:**

Wheeler et al. substantially teach the method according to claim 20. Not explicitly disclosed is further comprising: d) accessing a digital certificate previously associated with the financial account number, wherein the digital certificate includes a public key that corresponds to the private key, wherein the public key is capable of being used to validate the digital signature; and e) enabling the digital certificate to be associated with the electronic document. However, Randle et al. teach that customers can gain access to resources by using a certificate related to the account (col. 11, lines 20-38). Furthermore, it is well known that a certificate is used to bind an identity to a public key. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to be able to access a digital certificate associated with the account in order to authenticate the entity's digital signature and to further associate the electronic document with that certificate. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Randle et al. suggest the use of an account certificate in order to gain access to an account-related services in col. 11, lines 20-38.

**VII. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wheeler et al., United States Pub. No. 2002/0026575 as applied to claim 20 above, and further in view of Meurer, United States Patent Application Publication No. 2004/0215566.**

**As per claim 24:**

Wheeler et al. substantially teach the method, as applied to claim 20 above. Furthermore, Wheeler et al. teach the method, further comprising: d) receiving a second financial account number from the automated transaction machine (par. 118). Not explicitly disclosed is the method further comprising, e) assessing a processing fee associated with the digital signing of the electronic document to a financial account associated with the second financial account number. However, Meurer teaches assessing a processing fee collected for processing transactions (par. 13). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Wheeler et al. to cause a digital signature processing fee to be assessed to a financial account in response to producing the digital signature for the electronic document. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Meurer suggests assessing a processing fee for various transactions in paragraph 13.

**Reference Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. United States Patent No. 5,650,604, as well as United States Patent No. 6,098,053 are cited because they are relevant due to the manner in which the invention has been claimed.

**(10) Response to Argument**

**<u>Regarding Effective Filing date of the Wheeler Publication:</u>**

Appellants contend that the Wheeler Publication does not qualify as prior art under 35 U.S.C. § 103(a). Examiner respectfully disagrees. The Examiner (in the previously issued non-final office action) showed where each of the paragraphs/elements used from Wheeler were supported by the Wheeler Provisional Application (60/223076). The provisional application of Wheeler et al. was filed on

August 4, 2000 and therefore does qualify as prior art. Below, the Examiner has included where each paragraph cited from the Wheeler Publication is supported by the Wheeler Provisional Application and why it is supportive:

As per Paragraph [108]:

The Wheeler et al. portion relied upon in lines 4-9, "***In general a method in accordance with the first aspect of the present invention electronically communicating a message over a communications medium regarding an account that is associated with a public key, the corresponding private key of which is used to digitally sign the message,***" is supported on pages 5-6 of the "Aads" portion of the provisional which describes using a public key in association with a financial account, where a public key always has a corresponding private key used to provide a digital signature (See the last paragraph on page 5 to bottom of page 6 of "Aads").

The Wheeler et al. portion relied upon in lines 12-15, "***A method in accordance with the third aspect of the present invention includes maintaining a central database of information on all accounts associated with the same public key,***" is supported on pages 5-6 of the "Aads" portion of the provisional which describes that the financial institution registers a public key in association with each consumer's account to allow for the use of digital signatures. The financial infrastructure supports the registering public keys per consumer account which shows that there is a central database of information as cited (See the last paragraph on page 5 to bottom of page 6 of "Aads").

As per Paragraph [109]:

The Wheeler et al. portion relied upon in lines 1-5, "***As used herein, an "account holder" is generally any person possessing a device that is capable of generating a digital signature using a private key retained therein; the private key corresponding with a public key associated with an account upon which the person is authorized to act***," are supported on page 6 of the "Aads" portion of the provisional which describes a user/consumer using a public key in association with a financial account, where a public key always has a corresponding private key used to provide a digital signature (See the third paragraph of page 6 to the bottom of page 6 of "Aads").

The Wheeler et al. portion relied upon in lines 9-11, "***In some embodiments, the "account holder" is, itself, a device that is capable of generating a digital signature using a private key retained therein***," are supported on and on page 1 of the "Aadsstraw" portion of the provisional which describes that some type of supporting computing device performs the digital signing function on a message associated with, in one example, an account number (See second-to-last paragraph on page 1 of "Aadsstraw").

As per Paragraph [110] – [113]:

The Wheeler et al. portion relied upon in par. 113 lines 8-12, "***The account authority 212 comprises an entity or system that maintains one or more account databases, collectively referred to and illustrated by account database 214, which includes an account of the account holder 202***," is supported on page 6 of the "Rachip" portion of the provisional which describes using a database with two possible types of designs on how the public keys are to be registered with the consumer's account (See bullets 1-5 and the paragraph under the heading "PriMR Database Sizings on page 6 of "Rachip").

Furthermore, in par. 113 lines 12-18, "***Preferably, the account is identifiable within the account database 214 based on a unique identifier (acctID) 216, such as an account number. Further, the account authority 212 maintains an association between the account and the public key 218, which corresponds with the private key that is securely retained within the device 250 of the account holder 202***," is supported on pages 1-3 of the "Aadsstraw" portion of the provisional which describes that some type of supporting computing device performs the digital signing function on a message associated with, in one example, an account number (See second-to-last paragraph on page 1 to the end of the first paragraph on page 2 of "Aadsstraw"; Also see image labeled "base AADS chip" on page 3 of "Aadsstraw").

As per Paragraph [114]:

The Wheeler et al. portion relied upon in lines 6-16, "***Each communication is electronic, and each electronic communication ("EC") 206 from the account holder 202 to the account authority 212 includes an electronic message (M) that is digitally signed by the account holder 202 using the private key retained within the device 250. The means by which the device 250 communicates with the account authority 212 varies by the form factor of the device 250 and whether or not the device 250 is used in conjunction with a separate I/O support element (not shown) to assist in the generation or creation of the message, in the transmission***

***or communication of the EC to the account authority 212, or both***," are supported on page 5 of the "Aadsstraw" portion of the provisional which describes the use of a card which maintains a private key of a public/private key pair where that key pair is bound to a specific card, i.e. consumer, so that electronic communications from that user may be tracked/audited (See first and last paragraphs on page 5 of "Aadsstraw"). As per Paragraph [115]:

The Wheeler et al. portion relied upon in lines 1-10, "***The message preferably includes the unique identifier (acctID) 216 of the account of the account holder 202 and an instruction (i1) for the account authority 212 to perform in relation to the account. The digital signature of the message also preferably includes a unique random number or session key, such as, for example, a date and time stamp, so that no two digital signatures originated by the device 250 would ever be identical (and also so that any duplicate digital signature received by the account authority 212 could be identified as such and disregarded)***," are supported on pages 6 and 12-13 of the "Aadsstraw" portion of the provisional which describes an Account Authority Digital Signature which results in strong authentication by allowing for the use of session authentication, which may include date/time information to combat against replay attacks, for digital signatures and transaction authentications (See text under heading "AADS Replay Attack" on page 6 and bullets under "digital signature authentication" at the bottom of page 12 to the top of page 13 of "Aadsstraw"). These features are also supported on page 2 of the "Aadsbrnd" portion of the provisional which describes that the correct digital signature operation is enabled once the PIN is entered (See first paragraph and heading entitled "Enter PIN" on page 2 of "Aadsbrnd").

As per Paragraph [117]:

The Wheeler et al. portion relied upon in lines 1-5, "***Advantageously, since the unique identifier (acctID) 216 is all that must be included in the message in order for the account authority 212 to retrieve the appropriate public key 218 from the account database 214 for the purpose of authenticating the message and sender of the EC 206 and for having sufficient authorization from the account holder 202 for performing the instruction (i1) contained in the message, the account holder 202 need not include any 'identity' information in the message***," is supported on page 6 of the "Aads" portion of the provisional which describes that an account is bound to a public key (where the public key is a part of a public/private key pair) thus using an account number would allow the account authority to retrieve the public key which corresponds to that consumer's account, and further, authenticating that account holder. These features are also supported on page 1 of the "Aadsstraw" portion of the provisional which specifically describes that the message sent may be identified by an account number (See second-to-last paragraph on page 1 of "Aadsstraw").

The Wheeler et al. portion relied upon in lines 9-11, "***... the account authority 212 preferably will not perform any action on the account of the account holder 202 without a valid digital signature originated by the device 250 ...***" are supported on page 4 of the "Aadsstraw" portion of the provisional which describes that authenticating the user's identity is necessary and is checked because of the bindings of the public (& private) key to the account identifier, where it is known that if the signature information is not valid, operations are not to be performed. As per Paragraph [118]:

The Wheeler et al. portion relied upon in lines 1-38, "***FIG. 2a illustrates a plurality of possible relationships among the information contained within account database 214. Generally, each account within the database 214, for example, is identified by its account identifier (acctID) 216 and has associated therewith account information 240, such as information specific to the account holder (hereinafter 'customer-specific information') and information specific to the account (hereinafter 'account-specific information'), and public key information 218. At a minimum, the public key information 218 identifies each public key (PuK) associated with each particular account and/or account identifier 216. As shown, database 214 maintains a plurality of specific accounts 281,282,283,284,285,288, with a plurality of accounts (not shown but indicated by the '...') existing between accounts 285 and 288***" ... "***Each of these accounts 283,284 has the same account holder, who uses a single public key to access either or both of these accounts 283,284. Such a setup is beneficial, for example, when an account holder maintains a plurality of accounts (in this case, two) with a single account authority (e.g., primary and secondary bank accounts with the same financial institution)***," is supported on page 13 of the "Aadsstraw" portion of the provisional which describes multiple applications in correspondence with a public key and therefore the provisional supports multiple accounts associated with the public key (See bullets under the heading "digital signature binding" on page 13 of "Aadsstraw").

As per Paragraph [120]:

The Wheeler et al. portion relied upon in lines 1-13, "***Turning now to FIG. 2b, in a further feature of the present invention, account database 214 may also include Device Profile Information 270. Each Device Profile includes the Security Profile and transactional history of the device. The Security Profile includes the security features and manufacturing history of the device. The security features include those features of the device that protect the private key and other data within the device from discovery ('Security Characteristics') and features that perform entity authentication ('Authentication Capabilities'). Information contained in the Security Profile is described in greater detail herein in Section VI.4, entitled 'Applying Dynamic Risk Analysis to a Transaction'***," is supported on page 13 of the "Aadsstraw" portion of the provisional which describes an auditable key and binding registration process and audits maintained on a per transaction basis (See bullets under the headings "digital signature binding" and under "parameterized risk management based on audit trail associated with provable digital signature bindings, on per transaction basis..." on page 13 of "Aadsstraw").

As per Paragraph [129]:

The Wheeler et al. portion relied upon in lines 1-5, "***Of course, before either ABDS system 200,300 is utilized in practice, the account holder 202,302 first must establish an ABDS account with the appropriate account authority 212,312. The***

***steps involved in establishing a new ABDS account are set forth in FIGS. 4a and 4b***," is supported on page 6 of the "Aads" portion of the provisional which describes that the financial infrastructure must provide for a public key storage area per account record (See last two paragraphs on page 6 of "Aads"). These features are also shown on page 13 of the "Aadsstraw" portion of the provisional which describes authentication advances made available through the use of an Account Authority Digital Signature effort which includes account-based transactions in a financial infrastructure, i.e. transactions ranging from credit/debit to atm/echeck transactions (See text under the 3rd paragraph beginning with "The fundamental authentication advances provided by the Account Authority Digital Signature effort..." on page 13 of "Aadsstraw").

As per Paragraphs [130]-[131]:

The Wheeler et al. portions relied upon in lines 10-24, "***The account authority then obtains (Step 406) the public key from a device of the present invention and records (Step 408) the public key in the account database and associates it with the "shell" account or with the unique identifier. In some embodiments of the present invention, the unique identifier may actually be the public key from the device or a hashed version of the public key. The account authority then distributes or sends (Step 410) the device that retains the private key corresponding with the public key associated with the "shell" account to the prospective account holder with an offer to "open" an account on behalf of the prospective account holder with the account authority and with instructions for doing so. The account authority then waits for a response from the prospective***

***account holder***," is supported on page 3 of the "Aadsstraw" portion of the provisional which describes the use of a public key export mechanism within the chip held on the personal computing device (See first figure on page 3 of "Aadsstraw"). This feature is also supported on page 6 of the "Aadsstraw" portion of the provisional which describes strong signature validation by creating the signature in such a manner that it will not be subjected to a replay attack (See text under "AADS Replay Attack" and "Random Number Requirement" on page 6 of "Aadsstraw"). Finally, the feature is also shown on page 2 of the "Rachip" portion of the provisional which additionally incorporates a binding between the public key and the device (See first and second paragraphs on page 2 of "Rachip").

As per Paragraph [132]:

The Wheeler et al. portion relied upon in lines 1-12, "***If a response is received (Step 412), the account authority uses conventional authentication techniques to confirm that it is communicating with the prospective account holder. The account authority then obtains (Step 414) additional information, as needed, to populate the account record. The account authority then requires (Step 416) the prospective account holder to transmit a test message that is digitally signed using the device. Such test message confirms that the prospective account holder possesses the correct device. If the test message confirms, then the device is 'activated' (Step 418) for use with the associated account***," is supported on page 2 of "Aadsbrnd" portion of the provisional which describes that the correct PIN must be entered before the digital signature operation can be enabled (See text under heading "PIN –activated AADS devices" on page 2 of "Aadsbrnd"). This feature is also supported on page 6 of the "Aadsstraw" portion of the provisional which describes strong signature validation by creating the message/signature in a unique manner (See text under "AADS Replay Attack" on page 6 of "Aadsstraw").

As per Paragraph [145]:

The Wheeler et al. portion relied upon in lines 1-6, "***Preferably, the device is capable of receiving an electronic message and then originating a digital signature for the electronic message utilizing the private key stored therein. The device preferably also performs a hash function on the message received by the device prior to encryption with the private key***," are supported on page 1 of the "Aadsstraw" portion of the provisional which describes maintaining high integrity and using the private key to digitally sign an electronic message, where a secure hash is also performed on the message (See text under heading "AADS Chip Infrastructure" on page 1 of "Aadsstraw").

As per Paragraph [170]:

The Wheeler et al. portion relied upon in lines 1-12, "***Referring now to FIG. 76, an electronic communication (EC) 7601 in accordance with various aspects of the inventions described herein includes various data fields, elements, or portions, generally speaking, a message (M) 7603 and a digital signature (DS) 7605. These components generally form a data structure that may be stored, communicated, or otherwise manipulated with computing and communications apparatuses, according to the methods described herein. The EC 7601 may be included with,***

***and/or form a part of, a financial transaction in accordance with ISO Standard 8583, which is incorporated herein by reference, or an X9.59 transaction***," is supported on pages 3-6 of the "Aadsstraw" portion of the provisional which describe not only the use of an X9.59 transaction, but also that the system keeps an audit trail of transactions where each transaction comprises at least an electronic message and a signature (See figures and corresponding text on page 3, text under the heading "AADS Strawman Card Management" on page 4, the last paragraph beginning with "Also, in the AADS card management process..." on page 5, and the first paragraph under the heading "AADS Replay Attack" on page 6 of "Aadsstraw").

As per Paragraph [172]:

The Wheeler et al. portion relied upon in lines 1-13, "***According to a first arrangement of this aspect of the invention, the body portion 7609 comprises a message 7603 and the digital signature 7605 therefor (separated by a hashed line in the illustration). The message 7603 preferably includes an account identifier 7616 and message content 7618. The message content can include various types of information such as a further identifier, a command or instruction (i1) relating to the account, the public key (PuK) associated with the account, time/date stamp, encrypted message, and the like. The digital signature 7605 comprises information from the message 7603 (for example, a hash of the message, the message itself, or a compressed), signed with the sender's private key***," is supported on page 6 of the "Aadsstraw" portion of the provisional which describes that message identifiers, account identifiers, date/time stamping, and digital signatures are used in this infrastructure in order to prevent from a replay attack (See text under heading "AADS Replay Attack" on page 6 of "Aadsstraw").

As per Paragraph [182]-[183]:

The Wheeler et al. portion relied upon in lines 1-12 of par. 183, "***A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example, an account holder 602 comprising a person possesses a device in the form of a card 650, such as an IC card, credit card, or ATM card, which is capable of being used at an ATM machine 660 or the like. The card 650 securely protects therein a private key of a public-private key pair. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and a cash dispenser 668. The card 650 is associated with a debit or credit account maintained with an account authority comprising a financial institution 612***," is supported on page 3 of the "Aads" portion of the provisional which describes that the financial infrastructure includes a solution for networks that do not have face-to-face authentication, such as ATMs, which can take advantage of the strong binding of a public/private key pair to an entity having an account (See second paragraph beginning with "In that sense..." and first two paragraphs under the bullet "payload and certificate compression" on page 3 of "Aads").

Furthermore, par. 183 lines 12-18, "***The account may be a checking account, savings account, money market account, credit card account, or the like, and the financial institution may be a bank, savings and loan, credit card company, or the like. In this example, the ATM machine 660 communicates electronically with the***

***financial institution 612 over a secure, internal banking network 608***," is supported on page 6 of the "Aadsstraw" portion of the provisional which describes that the transmission of the data is secure by not only preventing from replay attacks, but also requiring the use of a random number in creating a secure hash of the message (See text under "AADS Replay Attack" and "Random Number Requirement" on page 6 of "Aadsstraw").

As per Paragraph [184]:

The Wheeler et al. portion relied upon in lines 4-6, "***With reference to FIG. 7, each account includes a unique account identifier comprising an account number 716***," is supported on page 5 of the "Aads" portion of the provisional which describes using the X9.59 consumer financial account-based payments which require a unique account identifier, i.e. account number (See first two paragraphs at the top of page 5 of "Aads").

Furthermore, lines 6-18 "***Each account number 716 identifies within the account database 614 account information 740, including customer-specific information 742 and account-specific information 744. In accordance with the present invention, the account number 716 also identifies public key information 718, which includes at least a public key of an account holder of the respective account. Also in accordance with a feature of the present invention, the account number 716 identifies device profile information 770 for the device that retains the private key corresponding with the public key associated with the account***," are supported on pages 13-14 of the "Aadsstraw" portion of the provisional which describes

X9.59 account-based financial transactions used for various transactions, including web transactions and ATM transactions, and employing a public/private key pair bound to the account and used for creating digital signatures (See text under headings "digital signature binding" and "parameterized risk management based on audit trail" and bottom of page 13 to page 14 of "Aadsstraw").

As per Paragraph [185]:

The Wheeler et al. portion relied upon in lines 1-11, "***In the example of FIG. 6, the customer-specific information 742 includes, for example, the name, address, social security number and/or tax-ID number of the account holder. The account-specific information 744 includes, for example, the current account balance, available credit, closing date and balance of current statement, and associated account identifiers. The public key information 718 of the account of the account holder 602 includes the public key corresponding to the private key retained within the card 650. The device profile information 770 includes information specific to the card 650***," is supported on pages 12-13 of the "Aadsstraw" portion of the provisional which describes maintaining passwords/PINS which are also forms of customer-specific information as well as using X9.59 for all account-based transactions where it is known that the customer's name and address are necessary for financial accounts (See page 12 to the top of page 13 of "Aadsstraw").

As per Paragraph [186]:

The Wheeler et al. portion relied upon in lines 1-5, "***As stated previously, an EC from the account holder 602 to the financial institution 612 may be used for three***

***different purposes: session authentication, transaction authentication, and transaction confirmation. In this business application, the most common type of EC is used merely for session authentication***," is supported on pages 12-13 of the "Aadsstraw" portion of the provisional which describes the use of session authentication, transaction authentication, and X9.59 for preserving the integrity, i.e. confirming a transaction, of the financial infrastructure (See from the bottom of page 12 to the top of page 13 of "Aadsstraw").

As per Paragraph [187]:

The Wheeler et al. portion relied upon in lines 1-17, "***Regardless of which type of EC is communicated from the account holder 602 to the financial institution 612, the basic methodology for composing and digitally signing the message (on the account holder end) and for authenticating the message and authenticating the entity (on the account authority end) is essentially the same. For example, turning now to FIG. 8, a transaction in accordance with the present invention is initiated (Step 802) in the implementation illustrated in FIGS. 6 and 7 when the account holder 602 inserts the card 650 into the card reader 664 of the ATM machine 660. The insertion of the card 650 initializes the ATM machine 660, which, using display 662, prompts (Step 804) the account holder 602 to perform entity authentication, such as providing a PIN, using the alphanumeric keypad 666. Once the PIN is input, an electronic message is composed (Step 806) for sending to the financial institution 612***," is supported on page 12 of the "Aadsstraw" portion of the provisional which describes the use of a form of PIN that must be entered by the customer to allow the transaction to occur (see top half of page 12 of "Aadsstraw"). This portion is also supported on page 13 which describes the use of ATMs which also require the customer to enter a PIN, where it is known that a keypad and some form of interface are inherent to an ATM so that transactions may be performed and validated visually by the customer in some manner (See lower half of page 13 of "Aadsstraw").

As per Paragraph [188]:

The Wheeler et al. portion relied upon in lines 1-8, is "***The ATM machine 660 displays a menu of available accounts upon which the account holder 602 may perform an action. The available accounts are stored within memory on the card 650 and retrieved by the ATM machine 660 for display to the account holder 602. Of course, if only one account is available in memory on the card 650, then that account is selected by default without requiring specific selection by the account holder 602***," supported on pages 4-5 of the "Aadsstraw" portion of the provisional which describes the use of a card which holds an account identifier as bound to the public/private key pair (See text under heading "AADS Strawman Card Management" on page 4 to the top of page 5 of "Aadsstraw").

As per Paragraph [189]:

The Wheeler et al. portion relied upon in lines 9-15, "***the ATM machine 660 composes an electronic message that includes an instruction to the financial institution 612 corresponding to the desired operation of the account holder 602. The electronic message also includes the account number 716 corresponding to***

***the account selected by the account holder 602***," is supported on page 1 of the "Aadsstraw" portion of the provisional which describes that the message is associated with an account number the type of operation must be specified in order to allow the operation to be performed (See text under the heading "AADS Chip Infrastructure" on page 1 of "Aadsstraw").

As per Paragraph [190]:

The Wheeler et al. portion relied upon in lines 1-8, "***The message then is transmitted (Step 808) to the card 650 for digital signing by the account holder 602. In this regard, upon receipt of data representing the message, the card 650 originates (Step 810) a digital signature for the message by first calculating a hash value for the data and then encrypting the hash value using the private key retained within the card 650. The card 650 then outputs (Step 812) the digital signature to the ATM machine 60, which then transmits (Step 814) the message and the digital signature therefor in an EC to the financial institution 612***," is supported on page 6 of the "Aadsstraw" portion of the provisional which describes that the transmission of the data is secure by not only preventing from replay attacks, but also requiring the use of a random number in creating a secure hash of the message (See text under "AADS Replay Attack" and "Random Number Requirement" on page 6 of "Aadsstraw"). The features are also supported on pages 1-2 of the "Aadsbrnd" portion of the provisional which describe how the key pair is generated and how the digital signature operation is performed in a transaction (See text under heading "Basic AADS chip functions" from page 1 to the top of page 2 of "Aadsbrnd").

In light of the above explanation of how each paragraph cited corresponds to and is supported by various portions of the provisional application, Examiner maintains that the provisional date of the Wheeler et al. Publication is the effective filing date. Furthermore, MPEP 901.04 states the following: "The 35 U.S.C. 102(e) date *>of a U.S. patent can be an earlier effective U.S. filing date. For example, the 35 U.S.C. 102(e) prior art date of a U.S. patent issued from< a nonprovisional application claiming the benefit of a prior provisional application (35 U.S.C. 111(b)) is the filing date of the provisional application >for subject matter that is disclosed in the provisional application<." The provisional application under question provides specific detail which "enables any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor of carrying out his invention," i.e. it allows one of ordinary skill in the art to derive a technical framework/system implementing the financial infrastructure disclosed in the provisional application (MPEP 601).

Furthermore, Examiner notes that some of the paragraphs cited are not only supported by the provisional, but also by the parent application 09/189,159 (now US Patent No. 6,820,202) of the Wheeler Publication which was filed on Nov. 9, 1998. (where the Wheeler Publication is a continuation-in-part of the parent application). Specific portions of US Patent No. 6,820,202 that show support for the paragraphs cited include the following: (1) The Background: column 1, lines 10-56, (2) The Summary: column 2, line 13 – column 3, line 18, and (3) Portions of the Detailed Description where these sections show support for binding accounts to an identity for non-face-to-face transactions (col. 1, lines 37-44); using digital signatures to validate messages (col. 1, lines 45-56 and col. 2, lines 19-28); the use of a public key to validate the digital signature (col. 2, lines 29-45), accounts having an associated encoding key (col. 2, lines 46-54), the use of digital signatures and the encoding key to validate electronic transactions (col. 2, line 55 – col. 3, line 7); use of a smart card or computer system may be used for implementing this system (col. 3, lines 8-13); using a PIN to allow a customer to continue to process a transaction (col. 4, lines 6-39); and allows for a terminal which dispenses cash (col. 4, lines 40-66).

## Rejection under 35 USC 103(a) over Wheeler in view of Cohen

**Regarding Claim 1, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "at least one data store includes a plurality of digital safe deposit accounts stored therein" and "each of the digital safe deposit accounts is associated with at least one private key." Examiner respectfully disagrees. Wheeler et al. teach that each account is associated with a public key in par. 113, lines 8-18: "*The **account authority 212 comprises an entity or system that maintains one or more account databases**, collectively referred to and illustrated by account database 214, which includes an account of the account holder 202. **Preferably, the account is identifiable within the account database 214 based on a unique identifier (acctID) 216, such as an account number. Further, the account authority 212 maintains an association between the account and the public key 218, which corresponds with the private key that is***

***securely retained within the device 250 of the account holder 202**.*" Since Wheeler et al. teach that each account is associated with a public key of a public/private key pair that means each account is also associated with the private key (since the public key is also associated with the private key). **The term "associated" is broad and therefore is broadly interpreted according to MPEP 2111.** Cohen was introduced because Wheeler et al. only discloses the use of accounts, as opposed to a "digital safe deposit account." Cohen suggests the use of an electronic safety deposit box to hold important documents on page 12, lines 7-14: "***The electronic safety deposit box is an online electronic lockbox associated with the webbank for storage, access, and recordkeeping of a user's important documents and assets. Accordingly, the user can easily and quickly access and present verified, digital copies of important documents and records from the central location, for self-access or presentation to third parties. Such documents can take advantage of date stamping, authentication, and other services provided by the metabank for providing security and trusted storage in online and traditional commercial transactions**.*" Cohen further discusses the use of electronic safety deposit boxes to maintain important records by a trusted party for record keeping purposes on page 22, paragraph 3: "*Functional parameters can also be set. These include parameters governing what functions the webbank can be used for. For example, some **webbanks may be set for funds storage, and/or withdrawals, and/or deposits**. Webbanks can also be set for association with programmable cards. **Webbanks can also be set for record keeping and presentation purposes, e.g. as electronic safety deposit boxes maintained by***

***a trusted neutral party (i.e. the metabank), for maintaining secure copies of important records, and for presentation of authenticated materials to third parties.*** *Similarly, webbanks can be set to hold public or private encryption keys and/or to serve as lower level certificate authorities under the metabank, which serves as a higher level authority. Webbanks can also be set as* ***transactional gatekeepers, serving the functions of bill and invoice generation and collection, including the collection of receipts corresponding to a user's transactions****. Any given function can be assigned to a webbank, including but not limited to one or more functions described in the present application.*" The motivation for combining the cited prior art to result in the electronic account from Wheeler et al. to be extended to a electronic safety deposit box is provided by Cohen as stated in the citation where Cohen suggests maintaining not only an electronic account, but a electronic safety deposit box which can keep secure copies of important records, in this case transactional information. Thus, the combination of Wheeler et al. and Cohen teach at least one data store includes a plurality of digital safe deposit accounts stored therein and where each of the digital safe deposit accounts is associated with at least one private key.

Appellant further contends that the Wheeler Publication and Cohen fail to teach/suggest "at least one data store in operative connection with the computer processor, wherein the at least on data store includes a plurality of digital safe deposit accounts stored therein; the computer processor is operative to communicate with a plurality of ATMs; [and] the computer processor operative responsive to at least one of the ATMs to cause a digital signature to be produced for an electronic document."

Examiner respectfully disagrees. The Examiner would first like to note that an element **"in operative connection"** or **"operative to communicate"** with another element in the broadest sense of those phrases (according to MPEP 2111) only require the capability of being connected and the capability of communicating. For example, a computer processor is in operative connection with a data store if the computer processor is somehow connected with an element that allows for a network connection. In reference to the limitations argued, Wheeler et al. teach a personal device that sends a message, which can be digitally signed with a private key associated with an account over a communications media, to a central database which maintains a plurality of accounts in paragraph 108, lines 4-18 and paragraph 109, lines 1-5: "*In general a method in accordance with the first aspect of the present invention* ***electronically communicating a message over a communications medium regarding an account that is associated with a public key, the corresponding private key of which is used to digitally sign the message.*** *A method in accordance with the third aspect of the present invention includes* ***maintaining a central database of information on all accounts associated with the same public key***" ... "*As used herein, an* ***'account holder' is generally any person possessing a device that is capable of generating a digital signature using a private key retained therein; the private key corresponding with a public key associated with an account upon which the person is authorized to act***." The previously cited portion shows that Wheeler et al. teach that an account is associated with both the public key and the corresponding private key, where the private key is used to create a digital signature, as well as a central database to maintain the plurality of accounts. Wheeler et al. further describe the disclosed system in reference to a Financial Institution Account where each customer has an IC card containing the private key (where the previously cited portion shows that the private key is used to perform digital signature operations) used in conjunction with an ATM which communicates with the financial institution, i.e. the central database of information holding the accounts in paragraph 183, lines 1-18 and paragraph 184, lines 4-6: "*A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example,* ***an account holder*** *602* ***comprising a person possesses a device in the form of a card*** *650,* ***such as an IC card, credit card, or ATM card, which is capable of being used at an ATM machine*** *660* ***or the like. The card*** *650* ***securely protects therein a private key of a public-private key pair****. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and a cash dispenser 668.* ***The card 650 is associated with a debit or credit account maintained with an account authority comprising a financial institution*** *612. The account may be a checking account, savings account, money market account, credit card account, or the like, and the financial institution may be a bank, savings and loan, credit card company, or the like. In this example, the* ***ATM machine*** *660* ***communicates electronically with the financial institution*** *612* ***over a secure, internal banking network*** *608.*"..."*With reference to FIG. 7,* ***each account includes a unique account identifier comprising an account number*** *716.*" Thus, Wheeler et al. teach that the card contains a processor, i.e. computer processor, and this card is in operative connection, i.e. the card connects to the ATM which allows it to be operatively connected through a network, to the data store, i.e. the central database of the financial institution which contains a plurality of accounts. Furthermore, Wheeler et al. teach that the card containing the computer processor is operative, i.e. capable of, communicating with a plurality of ATMs (depending on the ATM that it is inserted into). Finally, Wheeler et al. teach that the card with the integrated chip (i.e. processor) is operative to digitally sign an electronic document once the ATM has completed the transaction so that the signed transaction may be sent to the central database of the financial institution.

**Regarding Claim 2, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein the computer processor is operative to receive the electronic document from the at least one ATM, where the computer processor is operative to store the electronic document in the data store in association with the one digital safe deposit account." Examiner respectfully disagrees. Wheeler et al. teach that the electronic documents pertaining to various transactions may be maintained in storage in par. 170, lines 1-12: "***an electronic communication (EC) 7601 in accordance with various aspects of the inventions described herein includes various data fields, elements, or portions, generally speaking, a message (M) 7603 and a digital signature (DS) 7605. These components generally form a data structure that may be stored, communicated, or otherwise manipulated with computing and communications apparatuses, according to the methods described herein. The EC 7601 may be included with, and/or form a part of, a financial transaction in accordance with ISO Standard***

***8583, which is incorporated herein by reference, or an X9.59 transaction."*** Wheeler et al. suggest the storage of these documents in order to maintain a record of the transactional history for the customer. Thus, Wheeler et al. suggest wherein the computer processor is **operative to receive** the electronic document from the at least one ATM, where the computer processor is **operative to store** the electronic document in the data store in association with the one digital safe deposit account.

**Regarding Claim 3, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein the computer processor is operative to retrieve the electronic document from the data store and send the electronic document to any one of the plurality of ATMs." Examiner respectfully disagrees. Cohen teaches that the documents are maintained in a manner that allows for quick and easy access on page 12, lines 7-14: "***The electronic safety deposit box is an online electronic lockbox associated with the webbank for storage, access, and recordkeeping of a user's important documents and assets. Accordingly, the user can easily and quickly access and present verified, digital copies of important documents and records from the central location, for self-access or presentation to third parties. Such documents can take advantage of date stamping, authentication, and other services provided by the metabank for providing security and trusted storage in online and traditional commercial transactions***." Thus, Cohen suggests a computer processor **operative to retrieve** the electronic document from the data store and send it to a plurality of ATMs.

**Regarding Claim 4, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. fail to teach/suggest "wherein the computer processor is operative to encrypt and decrypt the electronic document stored in the at least one data store responsive to a secret key received from the at least one ATM." Examiner respectfully disagrees. Wheeler et al. teach that the electronic documents pertaining to various transactions may be maintained in storage where the documents are encrypted and decrypted in various stages of the transaction in par. 117, lines 1-5: "***Advantageously, since the unique identifier (acctID) 216 is all that must be included in the message in order for the account authority 212 to retrieve the appropriate public key 218 from the account database 214 for the purpose of authenticating the message and sender of the EC 206 and for having sufficient authorization from the account holder 202 for performing the instruction (i1) contained in the message, the account holder 202 need not include any 'identity' information in the message***." Wheeler et al. further suggest the following in paragraph 172, lines 1-13: "*According to a first arrangement of this aspect of the invention, the body portion 7609 comprises a message 7603 and the digital signature 7605 therefor (separated by a hashed line in the illustration).* ***The message 7603 preferably includes an account identifier 7616 and message content 7618. The message content can include various types of information such as a further identifier, a command or instruction (i1) relating to the account, the public key (PuK) associated with the account, time/date stamp, encrypted message, and the like.*** *The digital signature 7605 comprises information from the message 7603 (for example, a hash of the message, the message itself, or a compressed), signed with the sender's* *private key.*" Thus, Wheeler et al. teach wherein the computer processor is **operative to** encrypt and decrypt the electronic document stored in the at least one data store responsive to a secret key received from the at least one ATM.

**Regarding Claim 5, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein each digital safe deposit account is associated with a financial account number, wherein the computer processor is operative to access the private key associated with the one digital safe deposit account responsive to a message received from the at least one ATM which includes a financial account number that corresponds to the financial account number associated with the one digital safe deposit account." Examiner respectfully disagrees. Wheeler et al. teach that each of the accounts are identified by a unique account number within the financial institution, where the computer processor accesses the private key in order to digitally sign the message received from an ATM in par. 189, lines 9-15 and par. 190, lines 1-8: "***the ATM machine 660 composes an electronic message that includes an instruction to the financial institution 612 corresponding to the desired operation of the account holder 602. The electronic message also includes the account number 716 corresponding to the account selected by the account holder 602.***"... "***The message then is transmitted (Step 808) to the card 650 for digital signing by the account holder 602. In this regard, upon receipt of data representing the message, the card 650 originates (Step 810) a digital signature for the message by first calculating a hash value for the data and then encrypting the hash value using the private key retained within the card***

***650. The card 650 then outputs (Step 812) the digital signature to the ATM machine 60, which then transmits (Step 814) the message and the digital signature therefor in an EC to the financial institution 612**.*" Thus, Wheeler et al. teach wherein each digital safe deposit account is associated with a financial account number, wherein the computer processor is **operative to** access the private key associated with the one digital safe deposit account responsive to a message received from the at least one ATM which includes a financial account number that corresponds to the financial account number associated with the one digital safe deposit account.

**Regarding Claim 6, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein the at least one financial account number corresponds to a credit card number." Examiner respectfully disagrees. Wheeler et al. teach many different types of accounts that can be addressed within this financial infrastructure in par. 183, lines 1-12: "*A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example, an account holder 602 comprising a person possesses a device in the form of a card 650, such as an IC card,* ***credit card****, or ATM card, which is capable of being used at an ATM machine 660 or the like. The card 650 securely protects therein a private key of a public-private key pair. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and a cash dispenser 668. The card 650 is associated with a debit or* ***credit account maintained with an account authority comprising a financial institution*** *612.*"

Thus, Wheeler et al. teach wherein the at least one financial account number corresponds to a credit card number.

**Regarding Claim 8, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein the computer processor is operative to maintain and store in the at least one data store, and access log in association with each digital safe deposit account." Examiner respectfully disagrees. Wheeler et al. teach that each account within a database contains a transactional history log which shows various accesses to the account in par. 120, lines 1-6: "*Turning now to FIG. 2b, in a further feature of the present invention,* ***account database 214 may also include Device Profile Information*** *270. Each Device Profile includes the Security Profile and* ***transactional history of the device****. The Security Profile includes the security features and manufacturing history of the device*." Thus, Wheeler et al. teach wherein the computer processor is **<u>operative to</u>** maintain and store in the at least one data store, and access log in association with each digital safe deposit account.

**Regarding Claim 9, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein the at least one ATM includes a cash dispenser, wherein the computer processor is operative through communication with a financial transaction processing system to cause a dispense of cash from the cash dispenser to be authorized." Examiner respectfully disagrees. Wheeler et al. teach an ATM with a cash dispenser where throughout the reference the IC card (i.e. the computer processor) maintains account information and enables the transaction to take place, i.e. without the card being present the cash cannot be dispensed from the ATM in par. 183, lines 1-12: "*A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example,* ***an account holder 602 comprising a person possesses a device in the form of a card 650, such as an IC card, credit card, or ATM card, which is capable of being used at an ATM machine*** *660 or the like. The* ***card 650 securely protects therein a private key of a public-private key pair****. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and* ***a cash dispenser 668. The card 650 is associated with a debit or credit account maintained with an account authority comprising a financial institution*** *612*." Thus, Wheeler et al. teach wherein the at least one ATM includes a cash dispenser, wherein the computer processor is operative through communication with a financial transaction processing system to cause a dispense of cash from the cash dispenser to be authorized.

**Regarding Claim 10, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein the computer processor is operative to cause a new digital safe deposit account to be created in the data store responsive to communication from the at least one ATM." Examiner respectfully disagrees. Wheeler et al. teach that each account is registered/created in the data store based on a communication from the computer processor inserted into the ATM in par. 129, lines 1-5; par. 131, lines 10-24; and par. 132 lines 1-12: "*Of course, before either ABDS system 200,300 is utilized in practice,*

***the account holder 202,302 first must establish an ABDS account with the appropriate account authority** 212,312. The steps involved in **establishing a new ABDS account** are set forth in FIGS. 4a and 4b*"… "*The account authority then **obtains (Step 406) the public key from a device of the present invention and records (Step 408) the public key in the account database and associates it with the "shell" account or with the unique identifier.** In some embodiments of the present invention, the unique identifier may actually be the public key from the device or a hashed version of the public key. The account authority then distributes or sends (Step 410) the device that retains the private key corresponding with the public key associated with the "shell" account **to the prospective account holder with an offer to "open" an account on behalf of the prospective account holder with the account authority and with instructions for doing so.** The account authority then waits for a response from the prospective account holder*"… "*If a response is received (Step 412), the account authority **uses conventional authentication techniques to confirm that it is communicating with the prospective account holder**. The account authority then obtains (Step 414) additional information, as needed, to **populate the account record. The account authority then requires (Step 416) the prospective account holder to transmit a test message that is digitally signed using the device. Such test message confirms that the prospective account holder possesses the correct device. If the test message confirms, then the device is 'activated'** (Step 418) **for use with the associated account.***" Thus, Wheeler et al.. teach wherein the computer processor is **<u>operative to</u>** cause a new digital safe deposit account to be created in the data store responsive to communication from the at least one ATM.

**Regarding Claim 11, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein the computer processor is operative to cause a new private key and a corresponding public key to be produced responsive to communication from the at least one ATM, wherein the computer processor is operative to store the private key in association with the new digital safe deposit account." Examiner respectfully disagrees. Wheeler et al. teach that each account created has a public/private key pair associated with it so that users of the account can be authenticated properly in par. 109, lines 1-11; and par. 113, lines 8-12: "*As used herein, an 'account holder' is generally any person possessing a* ***device that is capable of generating a digital signature using a private key retained therein; the private key corresponding with a public key associated with an account upon which the person is authorized to act***"..." *In some embodiments, the 'account holder' is, itself,* ***a device that is capable of generating a digital signature using a private key retained therein***"..." *The account authority 212 comprises an entity or system that* ***maintains one or more account databases, collectively referred to and illustrated by account database*** *214, which includes an account of the account holder 202."* Thus, Wheeler et al. teach wherein the computer processor is operative to cause a new private key and a corresponding public key to be produced responsive to communication from the at least one ATM, wherein the computer processor is operative to store the private key in association with the new digital safe deposit account.

**Regarding Claim 15, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein the computer processor is operative to receive a one-way hash of the electronic document from the at least one ATM, wherein the computer processor is operative to cause the digital signature to be generated responsive to the one-way hash and the private key." Examiner respectfully disagrees. Wheeler et al. teaches that the message is hashed and then the message can be digitally signed in par. 145, lines 1-6: "*Preferably, the device is capable of receiving an electronic message and then* ***originating a digital signature for the electronic message utilizing the private key stored*** *therein. The device preferably also* ***performs a hash function on the message*** *received by the device prior to encryption with the private key.*" Thus, Wheeler et al. teach wherein the computer processor is **operative to** receive a one-way hash of the electronic document from the at least one ATM, wherein the computer processor is **operative to** cause the digital signature to be generated responsive to the one-way hash and the private key.

**Regarding Claim 16, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein the computer processor is operative to cause a second digital signature to be produced for the electronic document responsive to a private key that is not associated with the one digital safe deposit account." Examiner respectfully disagrees. Wheeler et al.

suggest that many different accounts may be maintained by a single account holder and that each of those accounts must have the capability of being uniquely identified in par. 118, lines 3-34: "*Generally,* ***each account within the database 214, for example, is identified by its account identifier (acctID) 216 and has associated therewith account information 240, such as information specific to the account holder (hereinafter 'customer-specific information') and information specific to the account (hereinafter 'account-specific information'), and public key information 218****. At a minimum,* ***the public key information 218 identifies each public key (PuK) associated with each particular account and/or account identifier 216.*** *As shown, database 214 maintains a plurality of specific accounts 281,282,283,284,285,288, with* ***a plurality of accounts (not shown but indicated by the '...') existing between accounts*** *285 and 288*" ... "***Each of these accounts 283,284 has the same account holder, who uses a single public key to access either or both of these accounts*** *283,284.* ***Such a setup is beneficial, for example, when an account holder maintains a plurality of accounts (in this case, two) with a single account authority (e.g., primary and secondary bank accounts with the same financial institution)****.*" Wheeler et al. suggest the use of a unique account id per sub-account and that a public key may be associated with each individual account. Thus, Wheeler et al. suggest wherein the computer processor is **operative to** cause a second digital signature to be produced for the electronic document responsive to a private key that is not associated with the one digital safe deposit account.

**Regarding Claim 19, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. fail to teach/suggest "wherein the computer processor is operative to cause a digital time stamp to be produced and attached to the electronic document." Examiner respectfully disagrees. Wheeler et al. teach that the messages include information such as a date/time stamp in par. 172, lines 1-13: "*The message 7603 preferably includes an account identifier 7616 and message content 7618.* ***The message content can include various types of information*** *such as a further identifier, a command or instruction (i1) relating to the account, the public key (PuK) associated with the account,* ***time/date stamp****, encrypted message, and the like. The digital signature 7605 comprises information from the message 7603 (for example, a hash of the message, the message itself, or a compressed), signed with the sender's private key.*" Thus, Wheeler et al. teach wherein the computer processor is **operative to** cause a digital time stamp to be produced and attached to the electronic document.

**Regarding Claim 27, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine; wherein the request includes an account number that is associated with a digital safe deposit account; accessing a private key associated with the digital safe deposit account responsive to the account number; producing a digital signature for the electronic document visually displayed by the automated transaction machine; or causing a digital signature to be attached to the electronic document visually displayed by the automated transaction machine." Examiner respectfully disagrees. Wheeler et al. teaches that an ATM displays a menu of accounts associated with the account holder who has presented the card holding the private key to the ATM in par. 188, lines 1-5: "***The ATM machine 660 displays a menu of available accounts upon which the account holder 602 may perform an action. The available accounts are stored within memory on the card 650 and retrieved by the ATM machine 660 for display to the account holder 602.***" Since the account holder must choose and account number from the accounts displayed by an ATM and the system disclosed always signs the message containing the transaction as displayed by the ATM, with the account holder's card (i.e. the computer processor inserted into the ATM), the Examiner interprets this step as receiving a request from an ATM to sign the transaction message which was visually displayed step by step until the transaction is completed where the first step was choosing an account number and actually accessing the private key in order to enable the card to sign the transaction as visually displayed by the ATM. Wheeler et al. describe these steps in further detail in par. 189: "Upon selection of an account, **the ATM machine 660 displays a menu of operations that can be performed on the selected account. Such operations include, for example, money withdrawal, balance inquiry, statement request, money transfer, money deposit, bill payment, and the like**. Upon selection of the desired operation by the account holder 602, and after any additional information relating thereto is obtained from the account holder 602, such as a withdrawal or transfer amount and the like, ***the ATM machine 660 composes an electronic message that includes an instruction to the financial***

***institution 612 corresponding to the desired operation of the account holder 602. The electronic message also includes the account number 716 corresponding to the account selected by the account holder 602***." Once this message is created to properly depict the events of the transaction, the message is transmitted to the card for the digital signature process to occur in par. 190, lines 1-8: "***The message then is transmitted (Step 808) to the card 650 for digital signing by the account holder 602.*** *In this regard, upon receipt of data representing the message,* ***the card 650 originates (Step 810) a digital signature for the message by first calculating a hash value for the data and then encrypting the hash value using the private key retained within the card 650. The card 650 then outputs (Step 812) the digital signature to the ATM machine 60, which then transmits (Step 814) the message and the digital signature therefor in an EC to the financial institution 612***."

Furthermore, Cohen was introduced because Wheeler et al. only discloses the use of accounts, as opposed to a "digital safe deposit account." Cohen suggests the use of an electronic safety deposit box to hold important documents on page 12, lines 7-14: "***The electronic safety deposit box is an online electronic lockbox associated with the webbank for storage, access, and recordkeeping of a user's important documents and assets. Accordingly, the user can easily and quickly access and present verified, digital copies of important documents and records from the central location, for self-access or presentation to third parties. Such documents can take advantage of date stamping, authentication, and other services provided by the metabank for providing security and trusted storage in online and***

***traditional commercial transactions**.*" Cohen further discusses the use of electronic safety deposit boxes to maintain important records by a trusted party for record keeping purposes on page 22, paragraph 3: "*Functional parameters can also be set. These include parameters governing what functions the webbank can be used for. For example, some* ***webbanks may be set for funds storage, and/or withdrawals, and/or deposits****. Webbanks can also be set for association with programmable cards.* ***Webbanks can also be set for record keeping and presentation purposes, e.g. as electronic safety deposit boxes maintained by a trusted neutral party (i.e. the metabank), for maintaining secure copies of important records, and for presentation of authenticated materials to third parties.*** *Similarly, webbanks can be set to hold public or private encryption keys and/or to serve as lower level certificate authorities under the metabank, which serves as a higher level authority. Webbanks can also be set as* ***transactional gatekeepers, serving the functions of bill and invoice generation and collection, including the collection of receipts corresponding to a user's transactions****. Any given function can be assigned to a webbank, including but not limited to one or more functions described in the present application.*" The motivation for combining the cited prior art to result in the electronic account from Wheeler et al. to be extended to a electronic safety deposit box is provided by Cohen as stated in the citation where Cohen suggests maintaining not only an electronic account, but a electronic safety deposit box which can keep secure copies of important records, in this case transactional information.

Thus, the combination of Wheeler et al. and Cohen teach/suggests receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine; wherein the request includes an account number that is associated with a digital safe deposit account; accessing a private key associated with the digital safe deposit account responsive to the account number; producing a digital signature for the electronic document visually displayed by the automated transaction machine; and causing a digital signature to be attached to the electronic document visually displayed by the automated transaction machine.

**Regarding Claim 28, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "storing a digitally signed copy of the electronic document in a data store in association with the digital safe deposit account." Examiner respectfully disagrees. Wheeler et al. teach that the database maintains a transactional history per account in par. 170, lines 1-12: "*Referring now to FIG. 76, an electronic communication (EC) 7601 in accordance with various aspects of the inventions described herein includes various data fields, elements, or portions, generally speaking,* ***a message (M) 7603 and a digital signature (DS) 7605. These components generally form a data structure that may be stored,*** *communicated, or otherwise manipulated with computing and communications apparatuses, according to the methods described herein. The EC 7601 may be included with, and/or form a part of, a financial transaction in accordance with ISO Standard 8583, which is incorporated herein by reference, or an X9.59 transaction.*" Wheeler et al. further describe the concept of maintaining transactional history by the database in par. 120, lines 1-6: "*Turning now to FIG. 2b, in a further feature of the present invention,* ***account database 214 may also include Device Profile Information*** *270. Each Device Profile includes the Security Profile and* ***transactional history of the device****. The Security Profile includes the security features and manufacturing history of the device.*" Thus, Wheeler et al. teach storing a digitally signed copy of the electronic document in a data store in association with the digital safe deposit account.

**Regarding Claim 29, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein step (a) the account number corresponds to a financial account number." Examiner respectfully disagrees. Wheeler et al. teach many different types of accounts that can be addressed within this financial infrastructure in par. 183, lines 1-12: "*A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example, an account holder 602 comprising a person possesses a device in the form of a card 650, such as an IC card,* ***credit card, or ATM card****, which is capable of being used at an ATM machine 660 or the like. The card 650 securely protects therein a private key of a public-private key pair. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and a cash dispenser 668.* ***The card 650 is associated with a debit or credit account maintained with an account authority comprising a financial institution*** *612.*" Thus, Wheeler et al. teach wherein step (a) the account number corresponds to a financial account number.

**Regarding Claim 30, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "e) dispensing cash from the automated transaction machine." Examiner respectfully disagrees. Wheeler et al. teach an ATM with a cash dispenser where the card must be present to allow this transaction to take place in par. 183, lines 1-12: "*A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example, an account holder 602 comprising a person possesses a device in the form of a card 650, such as an IC card, credit card, or* ***ATM card, which is capable of being used at an ATM machine*** *660 or the like. The card 650 securely protects therein a private key of a public-private key pair. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and* ***a cash dispenser 668.*** *The card 650 is associated with a debit or credit account maintained with an account authority comprising a financial institution 612.*" Thus, Wheeler et al. teach e) dispensing cash from the automated transaction machine.

**Regarding Claim 33, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "responsive to the data associated with the financial account received [by at least one server] in (a), causing through operation of the at least one server, a private key which corresponds to the data associated with the financial account received in (a) to be accessed from at least one data store in operative connection with at least one server, wherein the private key was previously stored in the at least one data store in correlated relation with the data associated with the financial account; causing through operation of the at least one server, a digital signature to be produced for an electronic document responsive to the private key accessed; causing through operation of the at least one server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account." Examiner respectfully disagrees. Wheeler et al. teach that an account holder identifies and account he/she wishes to perform a transaction on in accordance with a public/private key pair which is associated with that account in par. 109, lines 1-11: "*As used herein, an* ***'account holder' is generally any person possessing a device that is capable of generating a digital signature using a private key retained therein; the private key corresponding with a public key associated with an account upon which the person is authorized to act.*** *In some embodiments, the 'account holder' is, itself, a device that is capable of generating a digital signature using a private key retained therein.*" In another embodiment directed to an ATM system disclosed, Wheeler et al. teach that an ATM displays a menu of accounts associated with the account holder who has presented the card holding the private key to the ATM in par. 188, lines 1-5: "***The ATM machine 660 displays a menu of available accounts upon which the account holder 602 may perform an action. The available accounts are stored within memory on the card 650 and retrieved by the ATM machine 660 for display to the account holder 602.***" The previous citation shows that Wheeler et al. suggests that the account holder must choose and account number from the accounts displayed by an ATM. Furthermore, the system disclosed by Wheeler et al. always digitally signs the message containing the transaction as displayed by the ATM, with the account holder's card (i.e. the computer processor inserted into the ATM). Thus, the Examiner interprets this as receiving, with an ATM, data associated with a financial account, where the ATM sends the displayed electronic document of the transaction to the card so the card may access the appropriately stored private key in the card's storage area (i.e. previously stored private key in the at least one data store in correlated relation with the data associated with the financial account), and enabling the card to digitally sign the transaction message (which was visually displayed step by step) with the private key accessed (i.e. causing through operation of the ATM a digital signature to be produced for an electronic document responsive to the private key accessed). Wheeler et al. describe these steps in further detail in par. 189: "*Upon selection of an account,* ***the ATM machine 660 displays a menu of operations that can be performed on the selected account. Such operations include, for example, money withdrawal, balance inquiry, statement request, money transfer, money deposit, bill payment, and the like.*** *Upon selection of the desired operation by the account holder 602, and after any additional information relating thereto is obtained from the account holder 602, such as a withdrawal or transfer amount and the like,* ***the ATM machine 660 composes an electronic message that includes an instruction to the financial institution 612 corresponding to the desired operation of the account holder 602. The electronic message also includes the account number 716 corresponding to the account selected by the account holder 602.***" As discussed, once this message is created to properly depict the events of the transaction, the message is transmitted to enable the card to perform the digital signature process in par. 190, lines 1-8: "***The message then is transmitted (Step 808) to the card 650 for digital signing by the account holder 602.*** *In this regard, upon receipt of data representing the message,* ***the card 650 originates (Step 810) a digital signature for the message by first calculating a hash value for the data and then encrypting the hash value using the private key retained within the card 650. The card 650 then outputs (Step 812) the digital signature to the ATM machine 60, which then transmits (Step 814) the message and the digital signature therefor in an EC to the financial institution 612***." Thus, these embodiments, which are both disclosed in the Wheeler et al. publication, were combined in order to allow for a combination of technical elements to yield a system with several beneficial aspects of the various embodiments as suggested by Wheeler et al. in par. 406: "***Many methods, embodiments, and adaptations of the present invention other than those herein described, as well as many variations, modifications, and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and the following detailed description thereof***, *without departing from the substance or scope of the present invention.* ***Furthermore, those of ordinary skill in the art will understand and appreciate that although steps of various processes may be shown and described in some instances as being carried out in a preferred sequence or temporal order, the steps of such processes are not necessarily to be limited to being carried out in such particular sequence or order. Rather, in many instances the steps of processes described herein may be carried out in various different sequences***

***and orders, while still falling within the scope of the present invention.*** *Accordingly, while the present invention is described herein in detail in relation to preferred methods and devices, it is to be understood that this detailed description only is illustrative and exemplary of the present invention and is made merely for purposes of providing a full and enabling disclosure of the invention."* Finally, Cohen was introduced in order to replace the ATM (as disclosed by Wheeler et al. in accordance with the steps discussed above) with a server suggested in Cohen in order to allow for an infrastructure that doesn't necessarily require an ATM, but allows for a server to carry out the disclosed operations shown on page 16, line 32 – page 17, line 5: "***A consumer can maintain his or her own webbank on a server, preferably the server of a financial institution****. This webbank is similar to a webpage of the prior art, but is further encoded with functionality to* ***serve as a miniature private bank which is a sub-bank of the overseer bank, known as a metabank****. This* ***webbank serves personal or corporate bank for receiving, transferring (e.g. at preprogrammed times and under preprogrammed conditions), managing, and monitoring information, funds, and transactions of the bank owner.***" The motivation for combining the cited prior arts to result in using a server in place of the ATM disclosed in Wheeler et al. is provided by Cohen as stated in the citation where Cohen suggests that webbanks may be maintained on a server of the financial institution where it can serve as a miniature private bank which is more easily accessible by the account holder than an ATM.

Thus, the combination of Wheeler et al. and Cohen teach/suggest responsive to the data associated with the financial account received [by at least one server] in (a), causing through operation of the at least one server, a private key which corresponds to the data associated with the financial account received in (a) to be accessed from at least one data store in operative connection with at least one server, wherein the private key was previously stored in the at least one data store in correlated relation with the data associated with the financial account; causing through operation of the at least one server, a digital signature to be produced for an electronic document responsive to the private key accessed; causing through operation of the at least one server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account.

**Regarding Claim 34, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein (a) the data associated with the financial account is representative of a financial account number." Examiner respectfully disagrees. Wheeler et al. teach many different types of accounts that can be addressed within this financial infrastructure in par. 183, lines 1-12: "*A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example, an account holder 602 comprising a person possesses a device in the form of a card 650, such as an IC card,* ***credit card, or ATM card****, which is capable of being used at an ATM machine 660 or the like. The card 650 securely protects therein a private key of a public-private key pair. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and a cash dispenser 668.* ***The card 650 is associated with a debit or credit***

***account maintained with an account authority comprising a financial institution*** *612.*" Thus, Wheeler et al. teach wherein (a) the data associated with the financial account is representative of a financial account number.

**Regarding Claim 35, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein (a) the at least one financial account number corresponds to at least one of a credit card number, a debit card number, and a bank account number." Examiner respectfully disagrees. Wheeler et al. teach many different types of accounts that can be addressed within this financial infrastructure in par. 183, lines 1-12: "*A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example, an account holder 602 comprising a person possesses a device in the form of a card 650, such as an IC card,* ***credit card, or ATM card****, which is capable of being used at an ATM machine 660 or the like. The card 650 securely protects therein a private key of a public-private key pair. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and a cash dispenser 668.* ***The card 650 is associated with a debit or credit account maintained with an account authority comprising a financial institution*** *612.*" Thus, Wheeler et al. teach wherein (a) the at least one financial account number corresponds to **at least one of** a credit card number, a debit card number, and a bank account number.

**Regarding Claim 36, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein (a) the data representative of the financial account number is received by the at least one server from an automated transaction machine in operative communication with the at least one server through a network, wherein (d) the automated transaction machine includes a display." Examiner respectfully disagrees. Wheeler et al. teach that a database receives a message with the account number from an ATM through a network in par. 114, lines 6-16, "***Each communication is electronic, and each electronic communication ("EC") 206 from the account holder 202 to the account authority 212 includes an electronic message (M) that is digitally signed by the account holder 202 using the private key retained within the device 250.*** *The means by which the device 250 communicates with the account authority 212 varies by the form factor of the device 250 and whether or not the device 250 is used in conjunction with a separate I/O support element (not shown) to assist in the generation or creation of the message,* ***in the transmission or communication of the EC to the account authority*** *212, or both.*" Wheeler et al. also teach that the public key used to verify the digitally signed message is found in the database by using the account ID, i.e. account number in par. 113, lines 12-18: "*Preferably, the* ***account is identifiable within the account database 214 based on a unique identifier (acctID) 216, such as an account number.*** *Further, the account authority 212 maintains an* ***association between the account and the public key 218, which corresponds with the private key*** *that is securely retained within the device 250 of the account holder 202.*" Wheeler et al. also teach that the ATM has a display in par. 183, lines 8-12: "***The ATM machine 660 includes a display 662****, a card reader 664, an alphanumeric keypad 666, and a cash dispenser 668. The card 650 is associated with a debit or credit account* *maintained with an account authority comprising a financial institution 612.*" Thus, Wheeler et al. teach wherein (a) the data representative of the financial account number is received by the at least one server from an automated transaction machine in operative communication with the at least one server through a network and wherein (d) the automated transaction machine includes a display.

**Regarding Claim 37, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "wherein (a) the automated transaction machine includes a cash dispenser." Examiner respectfully disagrees. Wheeler et al. also teach that the ATM has a cash dispenser in par. 183, lines 8-12: "***The ATM machine 660 includes*** *a display 662, a card reader 664, an alphanumeric keypad 666,* ***and a cash dispenser*** *668. The card 650 is associated with a debit or credit account maintained with an account authority comprising a financial institution 612.*" Thus, Wheeler et al. teach wherein (a) the automated transaction machine includes a cash dispenser.

**Regarding Claim 38, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "e) receiving with the at least one server, the electronic document; f) causing through operation of the at least one server the electronic document to be stored in the at least one data store in correlated relation with the data associated with the financial account received." Examiner respectfully disagrees. Wheeler et al. teach receiving the electronic document by the central database, i.e. server, where that server stores the document in association with the corresponding financial account in par. 170, lines 1-12:

"*Referring now to FIG. 76, an* ***electronic communication (EC) 7601 in accordance with various aspects of the inventions described herein includes various data fields, elements, or portions, generally speaking, a message (M) 7603 and a digital signature (DS)*** *7605. These* ***components generally form a data structure that may be stored****, communicated, or otherwise manipulated* ***with computing and communications apparatuses,*** *according to the methods described herein. The EC 7601 may be included with, and/or form a part of, a financial transaction in accordance with ISO Standard 8583, which is incorporated herein by reference, or an X9.59 transaction.*" Wheeler et al. further describe the concept of maintaining transactional history by the database in par. 120, lines 1-6: "*Turning now to FIG. 2b, in a further feature of the present invention,* ***account database 214 may also include Device Profile Information*** *270. Each Device Profile includes the Security Profile and* ***transactional history of the device****. The Security Profile includes the security features and manufacturing history of the device.*" Thus, Wheeler et al. teach e) receiving with the at least one server, the electronic document; f) causing through operation of the at least one server the electronic document to be stored in the at least one data store in correlated relation with the data associated with the financial account received.

**Regarding Claim 39, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "(g) subsequent to (f) receiving with at least one server, data associated with the financial account from a remote computer in operative communication with the at least one server through a network"..."(h) causing through operation of the at least one server the electronic document to be accessed from the at least on data store responsive to the data associated with the financial account received in (g)"..."(i) causing through operation of the at least one server, the electronic document to be communicated to the remote computer." Examiner respectfully disagrees. Wheeler et al. teach that the account authority database receives data associated with an account from an ATM through a network in par. 114, lines 6-16: "***Each communication is electronic, and each electronic communication ("EC") 206 from the account holder 202 to the account authority 212 includes an electronic message (M) that is digitally signed by the account holder 202 using the private key retained within the device 250****.* *The* ***means by which the device 250 communicates with the account authority 212 varies by the form factor of the device 250 and whether or not the device 250 is used in conjunction with a separate I/O support element (not shown) to assist in the generation or creation of the message, in the transmission or communication of the EC to the account authority*** *212****, or both****."*

Cohen further teaches allowing access to the documents in accordance with the account number received and communicating that document to the customer on page 12, lines 7-14: "***The electronic safety deposit box is an online electronic lockbox associated with the webbank for storage, access, and recordkeeping of a user's important documents and assets. Accordingly, the user can easily and quickly access and present verified, digital copies of important documents and records from the central location, for self-access or presentation to third parties. Such***

***documents can take advantage of date stamping, authentication, and other services provided by the metabank for providing security and trusted storage in online and traditional commercial transactions***."

Thus, Wheeler et al. and Cohen teach/suggest (g) subsequent to (f) receiving with at least one server, data associated with the financial account from a remote computer in operative communication with the at least one server through a network; (h) causing through operation of the at least one server the electronic document to be accessed from the at least on data store responsive to the data associated with the financial account received in (g); and (i) causing through operation of the at least one server, the electronic document to be communicated to the remote computer.

**Regarding Claim 41, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. and Cohen fail to teach/suggest "responsive to the data associated with the financial account received [by at least one server] in (a), causing through operation of the at least one server, a private key which corresponds to the data associated with the financial account received in (a) to be accessed from at least one data store in operative connection with at least one server, wherein the private key was previously stored in the at least one data store in correlated relation with the data associated with the financial account; causing through operation of the at least one server, a digital signature to be produced for an electronic document responsive to the private key accessed; causing through operation of the at least one server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account." Examiner respectfully disagrees. Wheeler et al. teach that an account holder identifies and account he/she wishes to perform a transaction on in accordance with a public/private key pair which is associated with that account in par. 109, lines 1-11: "*As used herein, an* ***'account holder' is generally any person possessing a device that is capable of generating a digital signature using a private key retained therein; the private key corresponding with a public key associated with an account upon which the person is authorized to act.*** *In some embodiments, the 'account holder' is, itself, a device that is capable of generating a digital signature using a private key retained therein.*" In another embodiment directed to an ATM system disclosed, Wheeler et al. teach that an ATM displays a menu of accounts associated with the account holder who has presented the card holding the private key to the ATM in par. 188, lines 1-5: "***The ATM machine 660 displays a menu of available accounts upon which the account holder 602 may perform an action. The available accounts are stored within memory on the card 650 and retrieved by the ATM machine 660 for display to the account holder 602.***" The previous citation shows that Wheeler et al. suggests that the account holder must choose and account number from the accounts displayed by an ATM. Furthermore, the system disclosed by Wheeler et al. always digitally signs the message containing the transaction as displayed by the ATM, with the account holder's card (i.e. the computer processor inserted into the ATM). Thus, the Examiner interprets this as receiving, with an ATM, data associated with a financial account, where the ATM sends the displayed electronic document of the transaction to the card so the card may access the appropriately stored private key in the card's storage area (i.e. previously stored private key in the at least one data store in correlated relation with the data associated with the financial account), and enabling the card to digitally sign the transaction message (which was visually displayed step by step) with the private key accessed (i.e. causing through operation of the ATM a digital signature to be produced for an electronic document responsive to the private key accessed). Wheeler et al. describe these steps in further detail in par. 189: "*Upon selection of an account,* ***the ATM machine 660 displays a menu of operations that can be performed on the selected account. Such operations include, for example, money withdrawal, balance inquiry, statement request, money transfer, money deposit, bill payment, and the like****. Upon selection of the desired operation by the account holder 602, and after any additional information relating thereto is obtained from the account holder 602, such as a withdrawal or transfer amount and the like,* ***the ATM machine 660 composes an electronic message that includes an instruction to the financial institution 612 corresponding to the desired operation of the account holder 602. The electronic message also includes the account number 716 corresponding to the account selected by the account holder 602***." As discussed, once this message is created to properly depict the events of the transaction, the message is transmitted to enable the card to perform the digital signature process in par. 190, lines 1-8: "***The message then is transmitted (Step 808) to the card 650 for digital signing by the account holder 602.*** *In this regard, upon receipt of data representing the message,* ***the card 650 originates (Step 810) a digital signature for the message by first calculating a***

***hash value for the data and then encrypting the hash value using the private key retained within the card 650. The card 650 then outputs (Step 812) the digital signature to the ATM machine 60, which then transmits (Step 814) the message and the digital signature therefor in an EC to the financial institution 612***." Thus, these embodiments, which are both disclosed in the Wheeler et al. publication, were combined in order to allow for a combination of technical elements to yield a system with several beneficial aspects of the various embodiments as suggested by Wheeler et al. in par. 406: "***Many methods, embodiments, and adaptations of the present invention other than those herein described, as well as many variations, modifications, and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and the following detailed description thereof***, *without departing from the substance or scope of the present invention.* ***Furthermore, those of ordinary skill in the art will understand and appreciate that although steps of various processes may be shown and described in some instances as being carried out in a preferred sequence or temporal order, the steps of such processes are not necessarily to be limited to being carried out in such particular sequence or order. Rather, in many instances the steps of processes described herein may be carried out in various different sequences and orders, while still falling within the scope of the present invention***. *Accordingly, while the present invention is described herein in detail in relation to preferred methods and devices, it is to be understood that this detailed description only is illustrative and exemplary of the present invention and is made merely for purposes of* *providing a full and enabling disclosure of the invention."* Finally, Cohen was introduced in order to replace the ATM (as disclosed by Wheeler et al. in accordance with the steps discussed above) with a server suggested in Cohen in order to allow for an infrastructure that doesn't necessarily require an ATM, but allows for a server to carry out the disclosed operations shown on page 16, line 32 – page 17, line 5: "***A consumer can maintain his or her own webbank on a server, preferably the server of a financial institution****. This webbank is similar to a webpage of the prior art, but is further encoded with functionality to* ***serve as a miniature private bank which is a sub-bank of the overseer bank, known as a metabank****. This* ***webbank serves personal or corporate bank for receiving, transferring (e.g. at preprogrammed times and under preprogrammed conditions), managing, and monitoring information, funds, and transactions of the bank owner.***" The motivation for combining the cited prior arts to result in using a server in place of the ATM disclosed in Wheeler et al. is provided by Cohen as stated in the citation where Cohen suggests that webbanks may be maintained on a server of the financial institution where it can serve as a miniature private bank which is more easily accessible by the account holder than an ATM.

Thus, the combination of Wheeler et al. and Cohen teach/suggest responsive to the data associated with the financial account received [by at least one server] in (a), causing through operation of the at least one server, a private key which corresponds to the data associated with the financial account received in (a) to be accessed from at least one data store in operative connection with at least one server, wherein the private key was previously stored in the at least one data store in correlated relation with the data associated with the financial account; causing through operation of the at least one server, a digital signature to be produced for an electronic document responsive to the private key accessed; causing through operation of the at least one server, the digital signature to be attached to the electronic document during or after the display of the electronic document through a display device viewable by a customer associated with the financial account.

**Rejection under 35 USC 103(a) over Wheeler in view of Cohen and Randle**

**Regarding Claim 7, 35 USC 103(a) Rejection:**

Appellants contend that Wheeler et al., Cohen, and Randle et al. fail to teach/suggest "wherein each digital safe deposit box is associated with at least one digital certificate, wherein the computer processor is operative to cause the digital signature and at least one of the digital certificates associated with the one digital safe deposit account to be attached to the electronic document." Examiner respectfully disagrees. Randle et al. was introduced because Randle et al. suggest the use of certificates to allow customers to gain access to an account, where it is well known that a public key appears within a certificate in col. 11, lines 20-38: "*As a master provider of utility services, the ECTS provides to member banks net settlements, real time payment verification, an account based routing service, hot file account services, acceptance mark services, certificate authority, audit and reporting service and protocols and messaging. In FIGS. 1A and 1B, the customer's bank 2* ***includes a real time payment system including the features of certificate management****, real time transaction management, on-us processing, real time account management, protocols, messaging* *and account databases, and a financial services gateway including the functions of applications management, transaction processing, certificate interface, service access management, application modules and the ECTS interface.* ***As shown, customer access to the ECTS member bank may be intranet or web-based or through kiosk terminals by way of an account certificate or through a personal ATM. ECTS also allows client application modules for individualized services.*** *"* The motivation for combining the cited prior arts to result in using certificates with the electronic safety deposit accounts (disclosed by the combination of Wheeler et al. and Cohen) is provided by Randle et al. as stated in the citation where Randle et al. suggest the use of an account certificate in order to gain access to an account-related services. Thus, the combination of Wheeler et al., Cohen, and Randle et al. teach/suggest wherein each digital safe deposit box is associated with at least one digital certificate, wherein the computer processor is operative to cause the digital signature and at least one of the digital certificates associated with the one digital safe deposit account to be attached to the electronic document.

**Regarding Claim 12, 35 USC 103(a) Rejection:**

Appellants contend that Wheeler et al., Cohen, and Randle et al. fail to teach/suggest "wherein the computer processor is operative to cause a digital certificate to be generated and stored in association with the new digital safe deposit account, wherein the digital certificate includes the public key." Examiner respectfully disagrees. Randle et al. was introduced because Randle et al. suggest the use of certificates to allow customers to gain access to an account, where it is well known that a public key appears within a certificate and these certificates must be stored to allow proper validation in col. 11, lines 20-38: "*As a master provider of utility services, the ECTS provides to member banks net settlements, real time payment verification, an account based routing service, hot file account services, acceptance mark services, certificate authority, audit and reporting service and protocols and messaging. In FIGS. 1A and 1B, the customer's bank 2* ***includes a real time payment system including the features of certificate management****, real time transaction management, on-us processing, real time account management, protocols,* ***messaging and account databases****, and a financial services gateway including the functions of applications management, transaction processing, certificate interface, service access management, application modules and the ECTS interface.* ***As shown, customer access to the ECTS member bank may be intranet or web-based or through kiosk terminals by way of an account certificate or through a personal ATM. ECTS also allows client application modules for individualized services****.*" The motivation for combining the cited prior arts to result in using certificates with the electronic safety deposit accounts (disclosed by the combination of Wheeler et al. and Cohen) is provided by Randle et al. as stated in the citation where Randle et al. suggest the use of an account certificate in order to gain access to an account-related services. Thus, the combination of Wheeler et al., Cohen, and Randle et al. teach/suggest wherein the computer processor is operative to cause a digital certificate to be generated and stored in association with the new digital safe deposit account, wherein the digital certificate includes the public key.

**Regarding Claim 13, 35 USC 103(a) Rejection:**

Appellants contend that Wheeler et al., Cohen, and Randle et al. fail to teach/suggest "wherein the computer processor is operative to receive a financial account number from the at least one ATM, wherein the computer processor is operative to store the financial account number in association with the new digital safe deposit account." Examiner respectfully disagrees. Wheeler et al. teach that the user chooses a particular account to operate on and that the card has these account numbers stored in par. 184, lines 4-18: "*With reference to FIG. 7,* ***each account includes a unique account identifier comprising an account number*** *716.* ***Each account number 716 identifies within the account database 614 account information 740, including customer-specific information 742 and account-specific information 744. In accordance with the present invention, the account number 716 also identifies public key information*** *718, which includes at least a public key of an account holder of the respective account. Also in accordance with a feature of the present invention,* ***the account number 716 identifies device profile information 770 for the device that retains the private key corresponding with the public key associated with the account.****"* Thus, Wheeler et al. teach wherein the computer processor is operative to receive a financial account number from the at least one ATM, wherein the computer processor is operative to store the financial account number in association with the new digital safe deposit account.

**Regarding Claim 14, 35 USC 103(a) Rejection:**

Appellants contend that Wheeler et al., Cohen, and Randle et al. fail to teach/suggest "wherein the computer processor is operative to receive a password input from the at least one ATM, wherein the computer processor is operative to store the password input in association with the new digital safe deposit account." Examiner respectfully disagrees. Wheeler et al. teach that a PIN or some type of password must be entered before a transaction can occur, and that there must be a way to validate the PIN entered against the actual PIN to determine if the user can be authenticated in par. 187, lines 1-17: "*Regardless of which type of EC is communicated from the account holder 602 to the financial institution 612, the* ***basic methodology for composing and digitally signing the message (on the account holder end) and for authenticating the message and authenticating the entity (on the account authority end) is essentially the same****. For example, turning now to FIG. 8, a transaction in accordance with the present invention is initiated (Step 802) in the implementation illustrated in FIGS. 6 and 7* ***when the account holder 602 inserts the card 650 into the card reader 664 of the ATM machine 660. The insertion of the card 650 initializes the ATM machine 660, which, using display 662, prompts (Step 804) the account holder 602 to perform entity authentication, such as providing a PIN, using the alphanumeric keypad 666. Once the PIN is input, an electronic message is composed (Step 806) for sending to the financial institution 612***." Thus, Wheeler et al. teach wherein the computer processor is operative to receive a password input from the at least one ATM, wherein the computer processor is operative to store the password input in association with the new digital safe deposit account.

**Regarding Claim 40, 35 USC 103(a) Rejection:**

Appellants contend that Wheeler et al., Cohen, and Randle et al. fail to teach/suggest "e) causing through operation of the at least one server at least one digital certificate associated with the private key to be accessed from the at least one data store, wherein the at least one digital certificate was previously stored in the at least one data store in correlated relation with the data associated with the financial account; and f) causing through operation of the at least one server, the at least one digital certificate to be attached to the electronic document during or after the display of the electronic document through the display device." Examiner respectfully disagrees. Randle et al. teach that customers can gain access to resources by using a certificate related to the account, where it is well known to maintain a public key within a digital certificate and these certificates must be stored to allow proper validation in col. 11, lines 20-38: "*As a master provider of utility services, the ECTS provides to member banks net settlements, real time payment verification, an account based routing service, hot file account services, acceptance mark services, certificate authority, audit and reporting service and protocols and messaging. In FIGS. 1A and 1B, the customer's bank 2* ***includes a real time payment system including the features of certificate management****, real time transaction management, on-us processing, real time account management, protocols,* ***messaging and account databases****, and a financial services gateway including the functions of applications management, transaction processing, certificate interface, service access management, application modules and the ECTS interface.* ***As shown, customer access to the ECTS member bank may be intranet or web-based or through kiosk terminals by way of an account certificate or***

***through a personal ATM. ECTS also allows client application modules for individualized services.***" The motivation for combining the cited prior arts to result in using certificates with the electronic safety deposit accounts (disclosed by the combination of Wheeler et al. and Cohen) is provided by Randle et al. as stated in the citation where Randle et al. suggest the use of an account certificate in order to gain access to an account-related services. Thus, the combination of Wheeler et al., Cohen, and Randle et al. teach/suggest e) causing through operation of the at least one server at least one digital certificate associated with the private key to be accessed from the at least one data store, wherein the at least one digital certificate was previously stored in the at least one data store in correlated relation with the data associated with the financial account; and f) causing through operation of the at least one server, the at least one digital certificate to be attached to the electronic document during or after the display of the electronic document through the display device.

**Rejection under 35 USC 103(a) over Wheeler in view of Cohen and Meurer**

**Regarding Claim 17, 35 USC 103(a) Rejection:**

Appellants contend that Wheeler et al., Cohen, and Meurer fail to teach/suggest "wherein the computer processor is operative to cause a digital signature processing fee to be assessed to a financial account in response to causing the digital signature to be produced for the electronic document." Examiner respectfully disagrees. Meurer was introduced because Meurer suggests collecting a processing fee for transactions that are processed in par. 13: "*There are billions of dollars of fees generated in this process.* ***These fees come in the form of surcharges and interchange fees****. The surcharge* *fees are disclosed to and paid by the consumer, typically whenever the consumer uses any ATM other than those of his own bank and requests a cash withdrawal. The surcharge fee is usually around $1.50/transaction. Interchange fees are invisible to the consumer and are credited to the owner of the ATM that acquired the transaction and paid by the bank that issued the card that was used to conduct the transaction. Interchange fees are usually around $0.50/transaction and are* ***frequently shared among the various parties involved in conducting the transaction, such as the transaction processor, the network processor and the ATM owner. Thus, there is usually a total of about $2.00 of revenue available from most cash withdrawal transactions****.*" The motivation for combining the cited prior arts to result in charging fees for digital signatures within an ATM system is provided by Meurer suggests that charging a fee for transactions performed via an ATM result in a large revenue. Thus, the combination of Wheeler et al., Cohen, and Meurer teach/suggest wherein the computer processor is operative to cause a digital signature processing fee to be assessed to a financial account in response to causing the digital signature to be produced for the electronic document.

**Regarding Claim 18, 35 USC 103(a) Rejection:**

Appellants contend that Wheeler et al., Cohen, and Meurer fail to teach/suggest "wherein the computer processor is operative to receive information about the financial account from the at least one ATM." Examiner respectfully disagrees. Wheeler et al. teach that the computer processor receives information about the transactions being performed on the financial account in order to digitally sign the information in par. 190, lines 1-8: "***The message then is transmitted (Step 808) to the card 650 for digital signing by the account holder 602***. *In this regard, upon receipt of data representing the message, the card 650 originates (Step 810) a digital signature for the message by first calculating a hash value for the data and then encrypting the hash value using the private key retained within the card 650.* ***The card 650 then outputs (Step 812) the digital signature to the ATM machine 60, which then transmits (Step 814) the message and the digital signature therefor in an EC to the financial institution 612***." Thus, Wheeler et al. teach wherein the computer processor is operative to receive information about the financial account from the at least one ATM.

**<u>Rejection under 35 USC 103(a) over Wheeler</u>**

**Regarding Claim 20, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. fail to teach/suggest "b) accessing a private key associated with the financial account number" and "c) enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key." Examiner respectfully disagrees. Wheeler et al. teach that when the IC card (or ATM card) is inserted into the ATM, a listing of the possible accounts are displayed in par. 188, lines 1-4, is "***The ATM machine 660 displays a menu of available accounts upon which the account holder 602 may perform an action. The available accounts are stored within memory on the card 650 and retrieved by the ATM machine 660 for display to the account holder 602***." Wheeler et al. further teach that once the particular account is selected, the transaction may occur and an electronic document is sent to the card so that it may be digitally signed using the private key stored on the card in par. 190, lines 1-8: "*The message then is transmitted (Step 808) to the card 650 for digital signing by the account holder 602.* ***In this regard, upon receipt of data representing the message, the card 650 originates (Step 810) a digital signature for the message by first calculating a hash value for the data and then encrypting the hash value using the private key retained within the card 650****. The card 650 then* ***outputs (Step 812) the digital signature to the ATM machine 60****, which then transmits (Step 814) the message and the digital signature therefor in an EC to the financial institution 612.*" In another aspect of that embodiment of Wheeler et al., an account number is sent from the automatic transaction machine in order to access a private key for carrying out the digital signature process of the transaction in par. 113, lines 12-18: "*Preferably, the account is identifiable within the account database 214 based on* ***a unique identifier (acctID) 216, such as an account number****.* ***Further, the account authority 212 maintains an association between the account and the public key 218, which corresponds with the private key that is securely retained within the device 250 of the account holder 202****.*" The motivation for combining the two of the embodiments disclosed in Wheeler et al. is to provide for a quick and easy way to uniquely access the proper private key for an account. Thus, Wheeler et al. teach/suggest b) accessing a private key associated with the financial account number and c) enabling an electronic document displayed by the automated transaction machine to be digitally signed with the private key.

**Regarding Claim 21, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. fail to teach/suggest "d) receiving a password from the automated transaction machine; and e) verifying that the password corresponds to a valid password previously associated with the financial account number." Examiner respectfully disagrees. Wheeler et al. teach that a PIN entered by a customer must be verified in association with the particular account before transactions may be performed in par. 187, lines 11-17: "***The insertion of the card 650 initializes the ATM machine 660, which, using display 662, prompts (Step 804) the account holder 602 to perform entity authentication, such as providing a PIN, using the alphanumeric keypad 666. Once the PIN is input, an electronic message is composed (Step 806) for sending to the financial institution 612***." Thus, Wheeler et al. teach d) receiving a password from the automated transaction machine; and e) verifying that the password corresponds to a valid password previously associated with the financial account number.

**Regarding Claim 23, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. fail to teach/suggest "d) storing a digitally signed copy of the electronic document in a digital safe deposit account in association with the financial account number." Examiner respectfully disagrees. Wheeler et al. teach storing the electronic documents in a data structure of the financial infrastructure in par. 170, lines 1-12: "*Referring now to FIG. 76, an* ***electronic communication (EC) 7601 in accordance with various aspects of the inventions described herein includes various data fields, elements, or portions, generally speaking, a message (M) 7603 and a digital signature*** *(DS) 7605. These* ***components generally***

***form a data structure that may be stored**, communicated, or otherwise manipulated with computing and communications apparatuses, according to the methods described herein. The EC 7601 may be included with, and/or **form a part of, a financial transaction in accordance with ISO Standard 8583, which is incorporated herein by reference, or an X9.59 transaction**.*" Thus, Wheeler et al. teach d) storing a digitally signed copy of the electronic document in a digital safe deposit account in association with the financial account number.

**Regarding Claim 25, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. fail to teach/suggest "d) enabling the electronic document to be digitally time stamped." Examiner respectfully disagrees. Wheeler et al. teach that the messages include information such as a date/time stamp in par. 172, lines 1-13: "*The message 7603 preferably includes an account identifier 7616 and message content 7618. **The message content can include various types of information** such as a further identifier, a command or instruction (i1) relating to the account, the public key (PuK) associated with the account, **time/date stamp**, encrypted message, and the like. The digital signature 7605 comprises information from the message 7603 (for example, a hash of the message, the message itself, or a compressed), signed with the sender's private key.*" Thus, Wheeler et al. teach d) enabling the electronic document to be digitally time stamped.

**Regarding Claim 26, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. fail to teach/suggest "e) dispensing cash from the automated transaction machine." Examiner respectfully disagrees. Wheeler et al. teach an ATM with a cash dispenser where the card must be present to allow this transaction to take place in par. 183, lines 1-12: "*A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example, an account holder 602 comprising a person possesses a device in the form of a card 650, such as an IC card, credit card, or* ***ATM card, which is capable of being used at an ATM machine*** *660 or the like. The card 650 securely protects therein a private key of a public-private key pair. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and* ***a cash dispenser 668.*** *The card 650 is associated with a debit or credit account maintained with an account authority comprising a financial institution 612.*" Thus, Wheeler et al. teach e) dispensing cash from the automated transaction machine.

**Regarding Claim 31, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. fail to teach/suggest "receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine; b) causing a digital signature and a digital time stamp to be produced for the electronic document; and c) causing the digital signature and the digital time stamp to be attached to the electronic document." Examiner respectfully disagrees. In one of the embodiments disclosed, Wheeler et al. teaches that an ATM displays a menu of accounts associated with the account holder who has presented the card holding the private key to the ATM in par. 188, lines 1-5: "***The ATM machine 660 displays a menu of available accounts upon which the account holder 602 may perform an action. The available accounts are stored***

***within memory on the card 650 and retrieved by the ATM machine 660 for display to the account holder 602.*** " Since the account holder must choose and account number from the accounts displayed by an ATM and the system disclosed always signs the message containing the transaction as displayed by the ATM, with the account holder's card (i.e. the computer processor inserted into the ATM), the Examiner interprets this step as receiving a request from an ATM to sign the transaction message which was visually displayed step by step until the transaction is completed where the first step was choosing an account number and actually accessing the private key in order to enable the card to sign the transaction as visually displayed by the ATM. Wheeler et al. describe these steps in further detail in par. 189: "*Upon selection of an account,* ***the ATM machine 660 displays a menu of operations that can be performed on the selected account. Such operations include, for example, money withdrawal, balance inquiry, statement request, money transfer, money deposit, bill payment, and the like****. Upon selection of the desired operation by the account holder 602, and after any additional information relating thereto is obtained from the account holder 602, such as a withdrawal or transfer amount and the like,* ***the ATM machine 660 composes an electronic message that includes an instruction to the financial institution 612 corresponding to the desired operation of the account holder 602. The electronic message also includes the account number 716 corresponding to the account selected by the account holder 602****.*" Once this message is created to properly depict the events of the transaction, the message is transmitted to the card for the digital signature process to occur in par. 190, lines 1-8:

"***The message then is transmitted (Step 808) to the card 650 for digital signing by the account holder 602.*** *In this regard, upon receipt of data representing the message,* ***the card 650 originates (Step 810) a digital signature for the message by first calculating a hash value for the data and then encrypting the hash value using the private key retained within the card 650. The card 650 then outputs (Step 812) the digital signature to the ATM machine 60, which then transmits (Step 814) the message and the digital signature therefor in an EC to the financial institution 612***." Wheeler et al., in another embodiment, teach that the messages include information such as a date/time stamp in par. 115, lines 1-10: "*The message preferably includes the unique identifier (acctID) 216 of the account of the account holder 202 and an instruction (i1) for the account authority 212 to perform in relation to the account.* ***The digital signature of the message also preferably includes a unique random number or session key, such as, for example, a date and time stamp, so that no two digital signatures originated by the device 250 would ever be identical*** *(and also so that any duplicate digital signature received by the account authority 212 could be identified as such and disregarded).*" Wheeler et al. also discuss the use of timestamps in par. 172, lines 1-13: "*The message 7603 preferably includes an account identifier 7616 and message content 7618.* ***The message content can include various types of information*** *such as a further identifier, a command or instruction (i1) relating to the account, the public key (PuK) associated with the account,* ***time/date stamp****, encrypted message, and the like. The digital signature 7605 comprises information from the message 7603 (for example, a hash of the message,* *the message itself, or a compressed), signed with the sender's private key."* Thus, these embodiments, which are both disclosed in the Wheeler et al. publication, were combined in order to allow for a combination of technical elements to yield a system with several beneficial aspects of the various embodiments as suggested by Wheeler et al. in par. 406: "***Many methods, embodiments, and adaptations of the present invention other than those herein described, as well as many variations, modifications, and equivalent arrangements, will be apparent from or reasonably suggested by the present invention and the following detailed description thereof****, without departing from the substance or scope of the present invention.* ***Furthermore, those of ordinary skill in the art will understand and appreciate that although steps of various processes may be shown and described in some instances as being carried out in a preferred sequence or temporal order, the steps of such processes are not necessarily to be limited to being carried out in such particular sequence or order. Rather, in many instances the steps of processes described herein may be carried out in various different sequences and orders, while still falling within the scope of the present invention****. Accordingly, while the present invention is described herein in detail in relation to preferred methods and devices, it is to be understood that this detailed description only is illustrative and exemplary of the present invention and is made merely for purposes of providing a full and enabling disclosure of the invention."* Thus, Wheeler et al. teach/suggest receiving a request from an automated transaction machine to digitally sign an electronic document visually displayed by the automated transaction machine;

b) causing a digital signature and a digital time stamp to be produced for the electronic document; and c) causing the digital signature and the digital time stamp to be attached to the electronic document.

**Regarding Claim 32, 35 USC 103(a) Rejection:**

Appellant contends that Wheeler et al. fail to teach/suggest "e) dispensing cash from the automated transaction machine." Examiner respectfully disagrees. Wheeler et al. teach an ATM with a cash dispenser where the card must be present to allow this transaction to take place in par. 183, lines 1-12: "*A first business application 600 implementing the two-party ABDS system 200 of FIG. 2 is illustrated in FIG. 6. In this example, an account holder 602 comprising a person possesses a device in the form of a card 650, such as an IC card, credit card, or* ***ATM card, which is capable of being used at an ATM machine*** *660 or the like. The card 650 securely protects therein a private key of a public-private key pair. The ATM machine 660 includes a display 662, a card reader 664, an alphanumeric keypad 666, and* ***a cash dispenser 668.*** *The card 650 is associated with a debit or credit account maintained with an account authority comprising a financial institution 612.*" Thus, Wheeler et al. teach e) dispensing cash from the automated transaction machine.

<u>**Rejection under 35 USC 103(a) over Wheeler in view of Randle**</u>

**Regarding Claim 22, 35 USC 103(a) Rejection:**

Appellants contend that Wheeler et al. and Randle et al. fail to teach/suggest "d) accessing a digital certificate previously associated with the financial account number, wherein the digital certificate includes a public key that corresponds to the private key, wherein the public key is capable of being used to validate the digital signature; and e) enabling the digital certificate to be associated with the electronic document." Examiner respectfully disagrees. Randle et al. was introduced because Randle et al. suggest the use of certificates to allow customers to gain access to an account, where it is well known that a public key appears within a certificate and these certificates must be stored to allow proper validation in col. 11, lines 20-38: "*As a master provider of utility services, the ECTS provides to member banks net settlements, real time payment verification, an account based routing service, hot file account services, acceptance mark services, certificate authority, audit and reporting service and protocols and messaging. In FIGS. 1A and 1B, the customer's bank 2* ***includes a real time payment system including the features of certificate management****, real time transaction management, on-us processing, real time account management, protocols,* ***messaging and account databases****, and a financial services gateway including the functions of applications management, transaction processing, certificate interface, service access management, application modules and the ECTS interface.* ***As shown, customer access to the ECTS member bank may be intranet or web-based or through kiosk terminals by way of an account certificate or through a personal ATM. ECTS also allows client application modules for individualized services****.*" The motivation for combining the cited prior arts to result in using certificates with the electronic account is provided by Randle et al. as stated in the citation where Randle et al. suggest the use of an account certificate in order to gain access to an account-related services. Thus, the combination of Wheeler et al. and Randle et al. teach/suggest d) accessing a digital certificate previously associated with the financial account number, wherein the digital certificate includes a public key that corresponds to the private key, wherein the public key is capable of being used to validate the digital signature; and e) enabling the digital certificate to be associated with the electronic document.

**Rejection under 35 USC 103(a) over Wheeler in view of Meurer**

**Regarding Claim 24, 35 USC 103(a) Rejection:**

Appellants contend that Wheeler et al. and Meurer fail to teach/suggest "d) receiving a second financial account number from the automated transaction machine " and "e) assessing a processing fee associated with the digital signing of the electronic document to a financial account associated with the second financial account number." Examiner respectfully disagrees. Wheeler et al. teach that each account may contain more than one account number for various types of accounts in par. 118: "*FIG. 2a illustrates a plurality of possible relationships among the information contained within account database 214. Generally, **each account within the database 214, for example, is identified by its account identifier (acctID) 216 and has associated therewith account information 240, such as information specific to the account holder (hereinafter 'customer-specific information') and information specific to the account (hereinafter 'account-specific information'),** and public key information 218. At a minimum, the public key information 218 identifies each public key (PuK) associated with each particular account and/or account identifier 216. As shown,* *database 214 maintains a plurality of specific accounts 281,282,283,284,285,288, with a plurality of accounts (not shown but indicated by the '...') existing between accounts 285 and 288"* ... "***Each of these accounts 283,284 has the same account holder, who uses a single public key to access either or both of these accounts 283,284. Such a setup is beneficial, for example, when an account holder maintains a plurality of accounts (in this case, two) with a single account authority (e.g., primary and secondary bank accounts with the same financial institution)***."

Furthermore, Meurer was introduced because Meurer suggests collecting a processing fee for transactions that are processed in par. 13: "*There are billions of dollars of fees generated in this process.* ***These fees come in the form of surcharges and interchange fees****. The surcharge fees are disclosed to and paid by the consumer, typically whenever the consumer uses any ATM other than those of his own bank and requests a cash withdrawal. The surcharge fee is usually around $1.50/transaction. Interchange fees are invisible to the consumer and are credited to the owner of the ATM that acquired the transaction and paid by the bank that issued the card that was used to conduct the transaction. Interchange fees are usually around $0.50/transaction and are* ***frequently shared among the various parties involved in conducting the transaction, such as the transaction processor, the network processor and the ATM owner. Thus, there is usually a total of about $2.00 of revenue available from most cash withdrawal transactions***." The motivation for combining the cited prior arts to result in charging fees for digital signatures within an ATM system is provided by Meurer suggests that charging a fee for transactions performed via an ATM result in a large revenue.

Thus, the combination of Wheeler et al. and Meurer teach/suggest d) receiving a second financial account number from the automated transaction machine and e) assessing a processing fee associated with the digital signing of the electronic document to a financial account associated with the second financial account number.

**(11) Related Proceeding(s) Appendix**

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Nadia Khoshnoodi

Nadia Khoshnoodi

Conferees

Eddie Lee

**EDDIE C. LEE**
**SUPERVISORY PATENT EXAMINER**

Emmanuel Moise

E. Moise